ROBERT E. BUSHNELL*†

HENRY M. ZYKORIE
JOSEPH G. SEEBER°
JOHN C. BROSKY°+*
DARREN R. CREW+*
RUY M. GARCIA-ZAMOR*†

MICHAEL D. PARKER
DANIEL A. GESELOWITZ, PH.D.
(REG. PATENT AGENTS)

† ADMITTED IN MARYLAND
° ADMITTED IN VIRGINIA
+ ADMITTED IN PENNSYLVANIA
* NOT ADMITTED IN D.C.

R. E. BUSHNELL
ATTORNEY AT LAW

THE INVESTMENT BUILDING
1511 K STREET, N.W., SUITE 425
WASHINGTON, D.C. 20005-1401
UNITED STATES OF AMERICA

INTELLECTUAL PROPERTY LAW

TELEPHONE (202) 638-5740
(202) 638-2011
FACSIMILE (202) 628-0755
FACSIMILE (202) 628-3835
(410) 747-0022
E-MAIL: 2064566@MCIMAIL.COM

December 22, 1998

- ❑ *U.S. Postal Service*
- ❑ *Via Local Courier*
- ❑ *Via International Courier*
- ❑ *Via Facsimile No.* _____
- ❑ *Via E-Mail Attachment*
- ❑ *Please Acknowledge Receipt*

The Assistant Commissioner of Patents
Washington, D.C. 20231

Attorney Docket: P55501

Sir:

Submitted herewith is the following patent application:

Inventor(s): En-Seung KANG and Jin-Young BYUN

Title: THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD THEREOF

Please find attached hereto an application for patent which includes: Specification and Abstract, Claims, and a certified copy of the foreign priority document identified below:

Verified Showing of Small Entity Status: NO

Drawings: Formal drawings, 17 sheets, Figures 1 through 23B

Claim of priority under 35 U.S.C. §119: **YES**

REPUBLIC OF KOREA Application No(s). 98-39808 and 98-39809 filed in Korea on 24 September 1998.

Fee (see formula below): **CHECK IS ENCLOSED**

Basic Fee $380/760	$760.00
Additional Fees:	
Total number of claims in excess of 20 49 times 9/18 (49X18)	$882.00
Number of independent claims	
in excess of 3: 13 times $39/78 (13X78)	$1,014.00
Multiple Dependent Claims 3 times $130/260 (3X260)	$780.00
An Assignment is likewise enclosed: Recording Fee $40 . .	$00.00
Filing Non-English specification	$ 0.00
TOTAL FEES FOR THE ABOVE APPLICATION	*$3,436.00*

Inventor(s): En-Seung KANG and Jin-Young BYUN

Title: THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD THEREOF

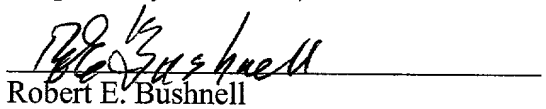
Should the enclosed check become lost or detached form the file, the Commissioner is authorized to charge Deposit Account No. 02-4943 for the fees incurred. Also, kindly charge any underpayment or credit any excess payment, and notify the undersigned attorney of any transaction regarding our Deposit Account accordingly.

In view of the above, it is requested that this application be accorded a filing date pursuant to 37 CFR 1.53(b).

Please address all correspondence to:

Robert E. Bushnell
1522 K Street, N.W.
Suite 300
Washington, D.C. 20005

Respectfully submitted,



Robert E. Bushnell
(Registration No. 27,774)

1522 K Street, N.W.
Suite 300
Washington, D.C. 20005-1202
Telephone: (202) 638-5740
Telefacsimile: (202) 628-0755

Filio: P55501
Date: December 22, 1998
REB/lj

PTO/SB/17 (2/98)
Approved for use through 9/30/2000. OMB 0651-0032
Patent and Trademark Office: U S DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL

Patent fees are subject to annual revision on October 1.
These are the fees effective October 1, 1997.
Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. *See* Forms PTO/SB/09-12.
See 37 C.F.R. §§1.27 and 1.28

Complete If Known	
Application Number	To be Assigned
Filing Date	December 22, 1998
First Named Inventor	En-Seong KANG
Examiner Name	To be Assigned
Group/Art Unit	To be Assigned
Attorney Docket No.	P55501

TOTAL AMOUNT OF PAYMENT	($) 3,476.00

METHOD OF PAYMENT (check one)

The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number: 02-4943
Deposit Account Number: _____

☐ Charge Any Additional Fee Required Under 37 C.F.R. §1.16 and 1.17

☐ Charge the Issue Fee Set in 37 C.F.R. §1.18 at the Mailing of the Notice of Allowance.

2. ■ Payment Enclosed:

■ Check ☐ Money Order ☐ Other
(CHECK No(s). 26437 and 26454)

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	790	201	395	Utility filing fee	$760.00
106	330	206	165	Design filing fee	$
107	540	207	270	Plant filing fee	$
108	790	208	395	Reissue filing fee	$
114	150	214	75	Provisional filing fee	$

SUBTOTAL (1) ($) 760.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total claims	69	20	49	x	18	=	$882
Independent Claims	16	3	13	x	78	=	$1,014
Multiple Dependent		3 x260				=	780.00

*** or number previously paid, if greater; For Reissues, see below*

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	22	203	11	**Claims in excess of 20**
102	82	202	41	**Independent claims in excess of 3**
104	270	204	135	**Multiple dependent claim, if not paid**
109	82	209	41	**** Reissue independent claims over original patent**
110	22	210	11	**** Reissue claims in excess of 20 and over original patent**

SUBTOTAL (2) ($) 2,676 .00

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge-late filing fee or oath	$
127	50	227	25	Surcharge-late provisional filing fee or cover sheet	$
139	130	139	130	Non-English specification	$
147	2,520	147	2,520	For filing a request for reexamination	$
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	$
113	1,840 *	113	1,840*	Requesting publication of SIR after Examiner action	$
115	110	215	55	Extension for reply within first month	
116	400	216	200	Extension for reply within second month	$
117	950	217	475	Extension for reply within third month	$
118	1,510	218	755	Extension for reply within fourth month	$
128	2,060	228	1,030	Extension for reply within fifth month	$
119	310	219	155	Notice of Appeal	$
120	310	220	155	Filing a brief in support of an appeal	$
121	270	221	135	Request for oral hearing	$
138	1,510	138	1,510	Petition to institute a public use proceeding	$
140	110	240	55	Petition to revive - unavoidable	$
141	1,320	241	660	Petition to revive - unintentional	$
142	1,320	242	660	Utility issue fee (or reissue)	$
143	450	243	225	Design issue fee	$
144	670	244	335	Plant issue fee	$
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	$
126	240	126	240	Submission of Information Disclosure Statement	$
581	40	581	40	Recording each patent assignment per property (Times number of properties)	$40 00
146	790	246	395	Filing a submission after final rejection (37 C.F.R. §1.129(a))	$
149	790	249	395	For each additional invention to be examined (37 C.F.R. §1.129(b))	$

Other Fee (specify) _____ $

Other Fee (specify) _____ $

** Reduced by Basic Filing Fee Paid **SUBTOTAL (3)**

SUBMITTED BY				Complete (if applicable)	
Typed or Printed Name	Robert E. Bushnell, Esq.			Reg. Number	27,774
Signature		Date	December 22, 1998	Deposit Account User ID	

REB/lj

THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD THEREOF

BACKGROUND OF THE DESCRIPTION

1. Field of the invention

The present invention is related to the encryption apparatus and the method thereof, and more particularly to the encryption apparatus and the method thereof which encrypts and transmits the digital content from the digital content transmission system by using the key information, the user key and the temporary validation key, to decrypt and replay the encrypted digital content in the user terminal by using the key information and the user authorization information.

2. Description of the Prior Art

Recently, people live in the midst of flood of information provided by various kinds of media such as broadcasting and press. This atmosphere created the information providers interested in providing the integrated information covering all the media and also there appeared users who want to selectively get a specific digital content out of the digital contents provided by the information provider (IP).

Accordingly, there appeared a digital content transmission system comprising the information providers who converts various information into the digital contents and stores this digital contents, and the users who are provided with this digital content from the IP by the network.

The digital content transmission system has provided an application program with easy downloadability of the digital contents. The user can get all the information he wants by accessing the digital content system through the network and using this application program.

The above mentioned digital contents are provided to the user for pay or for free. In case of the paid digital contents, the server with the digital content transmission system sets service fee. The service server charges the user according to the quantity of

used information when the charged digital content is downloaded to the user.

However, in case the user is connected to the server which provides the digital content commercially by the network, most of the users get an illegally copied and distributed digital content and this is very damaging to the server with a digital content transmission system.

SUMMARY OF THE INVENTION

The present invention is aimed at providing the digital content encryption apparatus and method thereof, which encrypts and transmitts the digital content from the digital content transmission system by using the key informtion, the user key and the temporary validation key, to decrypt and replay the encryted digital content in the user terminal by using the key information and the user authorization information.

Also, another purpose of this invention is to provide the digital content encryption communication protocol formed into a predetermined format for encryption of the digital content, according to which protocol the terminal unit decrypts the encrypted digital content.

To achieve the above-mentioned objects, a digital content encryption apparatus of the digital content transmission system comprises a terminal unit downloading and storing encryption key information requested by a user after the user registers member information including user's identity characters, said terminal unit decrypting a downloaded digital content using a decryption algorithm and the encryption key information to replay the digital content, and a service server generating the encryption key information corresponding to the identity characters from the terminal unit, said service server transmitting the encryption key information to the terminal unit, said service server encrypting the digital content using the encryption key information, said terminal unit downloading the encrypted digital content from the service server.

A digital content encryption apparatus of the digital content transmission system according to the present invention comprises a protocol format generator for generating a copyright protection protocol format, said protocol format generator generating a user key for encrypting a temporary validation key using a key generation algorithm

and key information, said key information being generated according to identity characters of a user, said protocol format generator generating a header using the user key to generate a temporary validation key, said generator adding encrypted digital content encrypted by the temporary validation key to the header to generate the copyright protection protocol format, and means for decrypting the copyright protection protocol format, said means receiving the generated copyright protection protocol format generated from the protocol format generator and then decrypting it using key information and a decryption algorithm to decrypt a user key and a temporary validation key, said means decrypting the encrypted digital content using the temporary validation key.

A protocol format for copyright protection of digital content according to the present invention includes a header field and an encrypted digital content field.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic block diagram showing one embodiment of the digital content encryption/decryption apparatus according to the present invention;

Fig. 2 is a drawing illustrating one embodiment of the terminal unit of Fig. 1;

Fig. 3 is a schematic block diagram showing another embodiment of the digital content encryption apparatus of Fig. 1;

Fig. 4 is a drawing illustrating one embodiment of the terminal unit of Fig. 3;

Fig. 5 is a block diagram showing the detailed functioinal sutructure of the digital content encryption apparatus of Fig. 1;

Fig. 6 is a block diagram showing the detailed functioinal sutructure of the digital content encryption apparatus of Fig. 3;

Fig. 7 is a flow chart illustrating the operation of the service server applied to Fig. 3;

Fig. 8 is a flow chart illustrating the operation of the host server applied to Fig. 3;

Fig. 9 is a schematic block diagram showing the functional structure of the digital content encryption apparatus according to the present invention;

Fig. 10 is an illustration of the protocol format applied to the present inven-

tion;

Fig. 11 shows another embodiment of the protocol format of Fig. 10;

Fig. 12 illustrates the header field applied to Fig. 10 and Fig. 11;

Fig. 13 shows another embodiment of the header field of Fig. 12;

Fig. 14 illustrates the unencrypted header field applied to Fig. 12 and Fig. 13;

Fig. 15 shows another embodiment of the unencrypted header field of Fig. 14;

Fig. 16 illustrates the detailed user authorization information applied to Fig. 14 and Fig. 15;

Fig. 17 is a drawing illustrating the detailed header field applied to Fig. 12 and Fig. 13;

Fig. 18 is a flow chart illustrating the method of generating the protocol applied to the present invention;

Fig. 19 is a flow chart illustrating the method of generating the header applied to Fig. 18;

Fig. 20 is a flow chart illustrating the method of generating the user authorization information applied to Fig. 19;

Fig. 21 is a flow chart illustrating the method of decrypting and replaying the encrypted digital contents according to the present invention;

Fig. 22 illustrates schematically the structure of the replaying device applied to Fig. 1 and Fig. 3; and

Fig. 23 is a flow chart illustrating the method of decrypting the encrypted digital contents.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention will now be described in detail referring to the accompanying drawings.

The present invention uses three keys in order to encrypt and decrypt the digital contents, which keys are explained below in detail.

First, key information is generated in the host server in response to the request of the service server when the user provided with the digital contents is unregistered.

The generated key information is stored in the user's terminal unit after transmitted through the service server.

In case of the digital content transmission system which combines the host server and the service server, the key information can be also generated in the service server.

The key information is used as means for getting a temporary validation key in the decryption process as well as in the encrytion process. Also, it is used as means for ascertaining whether the user is authrized to download and replay the encrypted digital contents in the user's terminal unit.

The key information is preferably generated by using random numbers and makes one-to-one correspondence with the user. Once generated, it is stored in the database of the host server with the user's characteritic charaters. The size of the key information is preferred to be 128 bytes.

Second, a user key is used for encrypting and decrypting the temporary validation key in the user authorization information of the header. It is generated by applying the forementioned key information to the key generation algorithm and used for generating and confirming the user's authorization information.

The user authorization information indicates a hash value of the user key generated by using the key information. When a hash value of the user key generated from the key information of the user proves the same as a hash value in the use authority of the header, the user is considered authrized to replay the encrypted digital contents.

To sum up, the user key is generated by using the key information and used for encryting the temporary validation key included into the user authorization information of the headerm. It is also used by the user to decrypt the encrypted temporary validation key, which is used to decrypt the encrypted digital contents.

Here the hash has features of always getting the same output from the same input and never inferring the input from the output, which features the present invention puts its basis on.

Third, a temporary validation key is used for encrypting a part of the digital contents and the header. It is preferably generated by using random numbers and its size

is determined to be a multiple of 8 bytes. It is preferred to be 8 byte in the present invention.

The temporary validation key has a feature that two temporary validation keys with the same content are not generated. For instance, the temporary validation key can be generated according to the time when the user accesses the service server. Accordingly, even the same user has the different temporary validation keys according to his access time. The temporary validation key exists valid only while the user accesses the system, that is, temporarily.

The present invention uses a plurality of algorithms, which include key generation algorithm, hash algorithm, and digital content encryption/decryption algorithm.

The key generation algorithm generates the user key by using the key information from the host server. In case of host server separate from service server, it is included in the service server.

The digital content encryption algorithm is also inclued in the service server and generates the header information to encrypt the digital contens.

The hash algorithm is used when the use autorization information is generated by using the user key in the service server or when it is ascertained whether the user is authorized.

To describe the digital content briefly, the digital content means a sort of data, e. g., music data, converted into digital signal which is stored in the form of a single file. The user can select the digital content stored in the form of file through the network access and read or listen to it by using a PC with an application program for communication or a replaying device connected to the PC.

The digital content includes all the information convertible into the digital data by the provider to be stored in the form of file, such as a magazine, a book, a dictionary and a drawing as well as a song.

Fig. 1 is a schematic block diagram showing one embodiment of the digital content encryption/decryption apparatus according to the present invention.

The terminal unit 10 transmits the user's identity characters and receives and stores the key information, which is generated in the service server 12 and corresponds

to the identity characters. It is also received from the service server 12 the protocol with the encrypted digital contents requested by the user, and decrypts and replays it by using the stored key information and the decryption algorithm.

The service server 12 generates the header with the user authorization information including the temporary validation key encrypted by the user key, and adds the encryted digital content to the header to generate the protocol for copyright protection. The protocol for copyright protection is transmitted to the user's terminal unit through network.

The terminal unit 10 is a personal computer (PC) 11a connected to the Internet. Also, the terminal unit 10 is applicable to any kind of apparatus equipped with a communication program for connection to the Internet. The good examples of the foregoing terminal unit 10 would be digital TV, cellular phone and web videophone. For example, the terminal unit with a network access program can be connected to a public switched telephone network or a wireless network.

Fig. 2 is a drawing illustrating one embodiment of the terminal unit of Fig. 1, where a terminal unit 10 is composed of a PC 11a equipped with the conventional communication device and a replaying device 11b. The PC 11a and replaying device 11b are provided with a plurality of decryption algorithm.

The PC 11a receives the key information from the service server 12 and stores it. Also, the PC 11a receives the protocol including the encrypted digital contents and records a storage medium such as HDD. It also generates the user key by using the stored key information, decrypts the temporary validation key by using the generated user key, and decrypts the encrypted digital contents by using the encrypted temporary validation key. As a result, the encrypted digital contents are replayed through a display or an audio device equipped by the PC 11a even without an additional replaying device 11b.

The replaying device 11b receives the key information and the encrypted digital contents from the PC 11a and decrypts the encrypted digital contents by using the stored decryption algorithm.

The replaying device 11b is either portable or stationary type according to the

type of the storage media.

The service server 12 generates key information corresponding to the identity characters transmitted from the terminal unit 10, stores the key information with the identity characters, and transmits it to the terminal unit in case the user requests the key information. The service server 12 generates the temporary validation key in response to the user's request, generates the user key by the key inforamtion, and generates the user authorization information from the temporary validation key encrypted by using the user key and a hash value of the user key. It also adds the digital contents encrypted by the encryption algorithm to the header with the user authorization information to form the copyright protection protocol and then transmits it to the terminal unit 10.

The service sanction agent server 14 receives the signal related to the digital content fees for downloading the digital content from the service server 12 and charges the user by accumulating the digital content fees of the registered user.

The identity characters are preferred to be the user's resident registration number, but any characters would be available only if they can identify the user like driver's license number.

Fig. 3 is a schematic block diagram showing another embodiment of the digital content encryption apparatus of Fig. 1. The explanation related to the terminal unit 20, the replaying device 21b and the service sanction agent server 24 will be omitted since they were described in the Fig. 1.

The service server 22 transmits to the host server 23 the request signal for the key information corresponding to the identity characters transmitted from the terminal unit 20. According to the request signal, the host server 23 transmits the key information to the service server, which key is then transmitted to the terminal unit 20.

Also, the service server 22 transmits the key information to the terminal unit 20 in response to the user's request. The service server 22 generates the temporary validation key in response to the user's request, generates the user key by the key inforamtion, and generates the user authorization information from the temporary validation key encrypted by using the user key and a hash value of the user key. It also adds the digital contents encrypted by the encryption algorithm to the header with the user authorization

information to form the copyright protection protocol and then transmits it to the terminal unit 20.

The host server 23 generates the key information corresponding to the identity characters transmitted from the service server 22 and stores it with the identity characters, then transmitting it to the service server 22 in response to the request signal of the service server 22.

In Fig. 1 and Fig. 3, the service server 12 and 22 can have a digital content list, with which the digital content provider can inform the user of the digital content he retains and the user is easy to select the digital content he wants. For example, the digital content list would be the title of the song, the name of singer etc. if the digital content is music data.

Fig. 5 is a block diagram showing the detailed functioinal structure of the digital content encryption apparatus of Fig. 1, where the functional structure of and the interrelation between the service server and the terminal unit are shown.

As shown in Fig. 5, the terminal unit 200 comprises an interface 201, a use authority identifier 202, a temporary validation key decryptor 203, and a digital content decryptor 204.

The interface 201 receives the key information generated corresponding to the user's identity characters. The use authority identifier 202 generates the user key after reading the header of the protocol received from the service server 210 and then identifies whether the user is authorized by analyzing the user authorization information with the generated user key. The temporary validation key decryptor 203 decrypts the temporary validation key using the user key. The digital content decryptor 204 decrypts the encrypted digital content using the temporary validation key decrypted by the temporary validation key decryptor 203.

The service server 210 comprises an interface 218, key information generator 212, a user key generator 213, a temporary validation key generator 214, a user authorization information generator 215, a header generator 216, and a protocol format generator 217.

The interface 218 receives the identity characters input from the terminal unit

200. The key information generator 212 determines whether the identity characters input from the interface 218 exist in the database 211, and then generates the key information. The user key generator 213 generates the user key by applying the key information to the key generation algorithm. The temporary validation key generator 214 generates the temporary validation key when the user accesses the service server 210 through the interface 218 and requests the digital contents. The user authorization information generator 215 generates the use authority key information by encrypting the temporary validation key using the user key generated by the user key generator 213 and then using the user key and the encrypted temporary validation key. The header generator 216 generates the header using the user authorization information and additional information necessary for encryption. The protocol format generator 217 generates the copyright protection protocol by adding the encrypted digital content to the header generated by the header generator 216.

The operation of the digital content encryption/decryption apparatus of Fig. 5 would be described below briefly.

When the user inputs the identity characters in order to get the digital contents from the service server 210, the service server 210 receives them through the interface 218 and outputs them to the key information generator 212.

Then, the key information generator 212 determines whether the identical ones with the input identity characters exist among the identity characters registered to the database 211. According to the result of determination, the key information generator 212 generates the new key information corresponding to the identity characters to transmit the key information to the user key generator 213 or transmits the registered key information to the user key generator 213.

The user key generator 213 generates the user key by applying the key information to the key generation algorithm and then outputs the user key to the key information generator 215.

The temporary validation key generator 214 generates the temporary validation key in response to the user access signal input through the interface 218 and inputs it to the key information generator 215.

The user authorization information generator 215 calculates the hash value by applying the user key to the hash algorithm, then encrypts the temporary validation key using the user key, and generates the user authorization information from a set of the hash value and the encrypted temporary validation key. The generated user authorization information is input to the header generator 216.

The header generator 216 adds the user authorization information to the header and then outputs it to the protocol format generator 217.

The protocol format generator 217 forms the protocol format by adding the encrypted digital content to the header and then transmits it to the terminal unit 200.

Fig. 6 is a block diagram showing the detailed functioinal structure of the digital content encryption apparatus of Fig. 3, where the functional structure of and the interrelation between the service server, the host server and the terminal unit are shown.

In Fig. 6, the key information generator 111 and the database 122 belong to the host server 120. Also, the user key generator 111, the interface 115, the temporary validation key generator 112, the user authorization information generator 113, the header generator 114, and the protocol format generator 114 belong to the service server 110. Description about the operation of each unit will be omitted, as the operation of each unit is the same as in case of Fig. 5.

In the above, the illustration of the present invention was made mostly referring to the PC user. However, it can be applicable to any kind of device equipped with a communication program and a decrytion algorithm.

Fig. 7 is a flow chart illustrating the operation of the service server applied to Fig. 3, which is related to the case the user unregistered to the service server intends to be provided with the digital contents.

The service server 22 can be accessed from the terminal unit 20 by the network access program. When the user inputs his identity characters, the service server identifies whether he is registered by comparing the input identity characters with the registered ones. If the user is registered, the key information is not generated additionally. If the input identity characters are determined not to exist in the service server 22, however, the service server 22 recognizes the user as a new member and proceeds into the mem-

bership registration.

If the user who wants to get the digital content makes the membership registration, the service server 22 receives the key information from the host server 23 and then transmits it to the terminal unit 20 in response to the user's request (S510).

The above mentioned key information generated in response to the identity characters is maintained valid unless the user applies the cancellation of his membership.

After the step of S510, the service server 22 determines whether the request signal for downloading the digital contents is received from the terminal unit 20 (S520). If the request signal for downloading is determined to be received, the service server 22 generates the user key using the key information, encrypts the temporary validation key using the user key, and then generates the header using the user key and the encrypted temporary validation key. It also generates the copyright protection protocol by adding the encrypted digital contents to the header and transmits the protocol to the user (S530).

After transmitting the digital content to the user, the service server 22 transmits the service fee information to the service sanction agent server 24 in order to add it to the stored service fee information. The service sanction agent server 24 charges the user for the digital content he used by using the service fee information.

Fig. 8 is a flow chart illustrating the operation of the host server applied to Fig. 3.

As shown in Fig. 8, the host server 23 determines whether the identity characters are received (S610).

When it is determined that the identity characters are received, the received characters are compared with the identity characters stored in the database to determine whether the identical identity characters exist (S620).

After the above step of S620, the key information stored with the identity characters are transmitted to the service server 22 when the identical identity characters are found (S630), while the key information is generated (S640) and then the generated key information is stored with the identity characters (S650) when the identical identity

characters are not found.

The step of S510 carried out by the service server 22 and the steps of S610 to S650 carried out by the host server 23 are carried out in case a service server 22 and a host server 23 are provided separately as in Fig. 2. When only a single service sever 11 is provided, however, the service server 11 integrally carries out the above mentioned steps to generate the key information corresponding to the user's identity characters and then transmit the generated key information to the user, which steps are not specifically described since the processes can be easily inferred from Fig. 7 & 8.

The terminal units 10 and 20 are provided with the key information and the digital contents, decrypts them through the stored decryption algorithm and at the same time outputs them to the external or internal audio output device to render them audible to the user.

Therefore, when illegal copying of the digital content from the terminal unit 10 and 20 to another terminal unit occurs, the absence of the key information within the other terminal unit will disable the encrypted digital content from being replayed and heard.

In case the registered user wants to provide another person with the digital contents, the identication charaters of the another person is stored with the identification charaters of the registered user. In thi case, the encrypted digital contents are decrypted and replayed with the former identification charaters as well as with the latter ones.

The fee for the provided digital contents would be paid by the user registered to the service server 22.

In the functional aspect, the digital content encryption/decryption apparatus according to the present invention can be divided broadly into the device encrypting the digital content and the device decrypting the encrypted digital content.

Fig. 9 is a schematic block diagram showing the functional structure of the digital content encryption apparatus according to the present invention.

The digital content encryption apparatus of the present invention consists of a protocol format generator 30 and a protocol format decoder 31.

The protocol format generator 30 generates the copyright protection protocol

format consisting of the encrypted digital contents and the header including the information necessary for encrypting and decrypting the digital contents. The protocol format decoder 31 decrypts and replays the encrypted digital contents from the copyright protection protocol format input from the protocol format generator 31 according to the header information of the protocol format.

More particularly, the protocol format generator 30 generates the user key by using the key information generated corresponding to the user's identity characters and the key generation algorithm. Then, it generates the header to which the user authorization information with the encrypted temporary validationkey is added using the user key and a hash value of the user key. It also generates the copyright protection protocol format by adding the encrypted digital content encrypted by the temporary validation key to the header.

The protocol format decoder 31 receives the copyright protection protocol format generated by the protocol format generator 30 to generate the user key using the key information, and decrypts the encrypted digital content using the temporary validation key after decrypting the temporary validation key using the user key in case the user is identified to be authorized. It is idenfied through the user authorization information which is achieved using the user key whether the user is authorized.

Operation of the protocol format processing system will be described in detail referring to the appended Fig. 10 and Fig. 16.

When the user selects the digital content he wants to be provided with, the digital content encryption apparatus of the present invention forms the digital content into the protocol format described below and then transmits it to the user.

Fig. 10 is an illustration of the protocol format applied to the present invention. The protocol for protecting the copyright of digital information comprises a header, which includes information for encrypting the digital contents and information for explaining the digital contens, and an encrypted digital content field.

The structure of the header will be described in detail referring to Fig. 5. The encrypted digital contents are encrypted partly by the user key and the temporary validation key so as not to replay in case of the absence of the key information.

Fig. 11, which illustrates another embodiment of the protocol format of Fig. 10, shows the copyright protection protocol including additional fields optionally added.

A field for indicating the size of an encrypted digital content is inserted between the header and the encrypted digital content field, which size is preferred to be the same as that of the unencrypted digital content field.

Also, the additional information field can be added to the rear end of the encrypted digital content field in order to define the encrypted digital contents for user's easy understanding.

In case the digital content is song data, for example, the additional information would be various data such as the singer, title of songs, playing time, title of albumn, the maker of albumn, publishing date, moving pictures of music video.

The additional information field is formed in a format that the header and the data are arranged in turnn, so it can be expanded regardless of the number of additional information.

Fig. 12 illustrates the header field of Fig. 10 and Fig. 11 more particularly, which comprises a copyright support information field, an unencrypted header field and an encrypted header field.

The copyright support information field includes the copyright support code showing whether the digital content provided by the digital content provider supports the copyright.

If the copyright support code exists in the copyright support information field, the digital contents provided to the user is recognized to be encrypted, and then decrypted to replay. Otherwise the digital content is recognized to be unencrypted and the decryption process is terminated in order for the digital contents to be replayed without decryption.

Fig. 13 shows another embodiment of the header field of Fig. 12. Fig. 11, which field includes optionally added additional fields.

An offset field and a field for indicating the size of the unencrypted header are inserted between the copyright support information field and the unencrypted header field. The offset field provides information on the position of the additional information

field, which enables the additional information field to be accessed without analysis of the header. Also, a field for indicating the size of the encrypted header is provided prior to the encrypted header field.

Fig. 14 illustrates the unencrypted header field applied to Fig. 12 and Fig. 13.

The unencrypted header field comprises a copyright library version field, a digital conversion format field for indicating the type of the digital conversion format, a key generation algorithm field for indicating the information on the key generation algorithm, a digital content encryption algorithm field for indicating the information on the digital content encryption algorithm, a field for indicating the user authorization information at PC, and a field for indicating the user authorization information at the replaying device.

The digital conversion format field shows in what conversion method the digital content is converted into the digital signal. Typical examples of the conversion method are MP3 and AAC.

The encryption algorithm field includes hash algorithm code, key encryption algorithm code, the size of initial vector (IV), the information on initial vector used for encrypting the digital contents.

The field for indicating the user authorization information at PC and the field for indicating the user authorization information at the replaying device are the most important in the header, which serve to identify the user's authority to use the digital cotents and increase in proportion to the number of peaple who share the encrypted digital contents.

Fig. 15, illustrating another embodiment of the unencrypted header field of Fig. 14, shows the unencrypted header field including optionally added additional fields.

A field for indicating the code of digital content provider is inserted between the digital content conversion format field and the key generation algorithm field. To the rear end of the digital content encryption algorithm field can be added a field of the number of users sharing the PC, a field of the number of users sharing the replaying device.

Fig. 16 illustrates the detailed structure of the user authorization information

fields applied to Fig. 14 and Fig. 15.

The user authorization information fields at PC and at the replaying device comprise a field for indicating the size of hash value generated by hash algorithm, a field for indicating a hash value of the user key, a field for indicating the size of resultant value of the encrypted temporary validation key generated by key encryption algorithm, and a field for indicating the resultant value of the encrypted temporary validation key.

Fig. 17 is a drawing illustrating the detailed header applied to Fig. 12 and Fig. 13.

The encrypted header field comprises a field for indicating the basic process unit of the digital contents, a field for indicating the number of the encrypted bytes, a field for indicating the encrypted frame unit, and a hash value field for determining the state of entire header.

The basic process unit of the digital contents and the number of the encrypted bytes can be assigned by the information provider. However, they are possibly set the basic values by a basic algorithm referring to the processing speed of a terminal unit and a memory.

A hash value in the hash value field indicates a hash value of both the copyright support information field and the unencrypted header field, i.e., a hash value of the fields prior to the encrypted header field within the header field.

Fig. 18 is a flow chart illustrating the method of generating the protocol applied to the present invention.

When the digital content request signal is input from the user, the temporary validation key is generated (S110). Then, it is determined whether the header generation algorithm defined by the digital content provider exists when the temporary validation key is generated (S120).

In case of existence of the header generation algorithm at the determination step of S120, the header is generated by the header generation algorithm defined by the digital content provider (S130). In case of non-existence of the header generation algorithm, the header is generated in a basic value (S190).

After the header is generated at the step of S130 or S190, the digital content is encrypted (S140) and then added to the header generated at the step of S130 or S190 (S150).

In case that the additional information is provided, it is determined whether the additional information to the digital contents combined with the header exists (S160). If the additional information is determined to exist at the step of S160, the additional information field is generated (S170) and added to the rear end of the encrypted digital content (S180) to form the copyright protection protocol. The copyright protection protocol is then transmitted to the user who want the digital contents.

The additional information to the digital contents is added optionally by the provider when the provider would like to make an additional explanation about the digital contents to the user. The additional information processing step of S220 can be added selectively by the service provider.

Fig. 19 is a flow chart illustrating the method of generating the header applied to Fig. 18.

The copyright support information field, describing whether the digital contents provided is under the protection of copyright, and a field for indicating the size of unencrypted header are generated and added to the header (S210). The unencrypted header field is also generated and added to the header (S220), which field includes the version information, a type of music, the code of service provider supporting the copyright, hash algorithm, key generation algorithm, and digital content encryption algorithm.

If the additional information field of the digital contents exists, information on the starting point of the additional information field can be also added to the header.

At step of S220 that a part of the header part is constructed, the user authorization information is generated using the key information the user has and the generated user authorization information is added to the header (S240). Following the step of S240, the encrypted header information is generated (S250).

The header information includes information necessary for encryption of the digital content such as size of the encrypted block, encryption period and encrypted

frame unit, etc. The header information is also generated to include the hash value by applying the whole header to the hash algorithm, with which value the change of header information can be determined.

The header information generated at the step of S250 is encrypted (S260) and then the information on the encrypted header and the size of the encrypted header is added to the header (S270), so that generated is the header added to the front end of the encrypted digital content transmitted to the user.

In case the encryption algorithm provided by the digital content provider exists (S260), the header information is encrypted by the encryption algorithm and the temporary validation key. Otherwise the header information is encrypted by the basic algorithm and the temporary validation key.

Fig. 20 is a flow chart illustrating the method of generating the user authorization information applied to Fig. 19, which describe in more detail the method of generating the encryption key information at the step of S230 of Fig. 19.

It is determined whether the key information or the temporary validation key exists (S310). The user key is generated by applying the key information to the key generation algorithm when it is determined that the key information and the temporary validation key exist at the step of S310 (S320).

A hash value is calculated by applying the user key generated at the step of S320 (S330) to hash algorithm, and then the temporary validation key is encrypted using the key encryption algorithm and the generated user key (S340). At the determination step of S310, the process is terminated with output of message of error when the key information or the temporary validation key is determined not to exist.

Fig. 21 is a flow chart illustrating the method of decrypting and replaying the encrypted digital contents according to the present invention.

First, it is determined whether the key information or the digital contents received from the digital content provider exists (S410). The header of the digital contents is read when either the digital content or the key information is determined to exist (S415), and the process is recognized to be an error and terminated when the digital contents and the key information do not exist (S480).

It is determined whether the header read at the step of S415 includes the copyright support code, that is to say, whether the digital content supports the copyright (S420).

If the copyright support code is determined to exist, the digital contents are recognized to be protected by copyright and the read unencrypted header information is stored at a memory as a predetermined variable (S425).

If the copyright support code is determined not to exist, that is, the digital contents are not protected by copyright, the digital contents is recognized to be an error in the decryption process. Then the decryption process is no longer carried out and the received digital contents are decoded and output, not passing through decryption process.

When the digital content is determined to be supported by copyright, the user key is generated using the key information and then the hash value of the generated user key is calculated (S430).

It is determined whether the calculated hash value of the user key is identical with a hash value of the user key in the header (S435).

When the calculated hash value of the user key is determined to coincide with the hash value of the user key in the header, the user is recognized to be authorized and the temporary validation key is decrypted using the user key (S440). The encrypted header is decrypted using the decrypted temporary validation key (S445). The hash value of entire header, which is served as a reference value for determination the change of entire header, is calculated by applying the entire header to hash algorithm (S450).

At the determination step of S435, the message of "Not authorized" is output and the entire digital content decryption process is terminated when the calculated hash value of the user key is determined not to be identical with the hash value of the user key in the header.

The change of the header is determined according to hash value of the entire header (S455). In case the header is determined not to be changed, the encrypted digital contents are decrypted (S455).

It is determined whether additional information exists (S465). The digital contents are replayed if the additional information is not determined not to exist (S470).

The additional information is processed and then replayed when the additional information is determined to exist (S475).

When the header is determined to be changed at the step of S455, the user is recognized not to be authorized so that the decryption process is terminated for the user not to replay the digital contents (S490).

Fig. 22 illustrates schematically the structure of the replaying device applied to Fig. 1 and Fig. 3.

Memory 300 includes a driving algorithm for the entire system and a plurality of algorithms for decrypting the encrypted digital contents. Memory 300 stores in itself the received key information and digital content data in response to the writing signal and outputs the stored key information and digital content data in response to the reading signal. Memory 300 is preferred to be a flash memory.

Microcomputer 320 receives the key information and digital content data to store memory 300, decrypts the encrypted digital contents by the algorithm stored in memory 300 and then outputs them according to the key signal input from the user key input device 330. At the same time, it controls display 340 to display the present state of the apparatus.

Microcomputer 320 generates the user key through the user authorization information of the header using the key information stored in memory 300 according to the algorithm, which is also stored in memory 300, when the input digital contents are encrypted. Also, microcomputer 320 decrypts the temporary validation key included in the user authorization information of the header using the generated user key. The encrypted digital contents are decrypted using the decrypted temporary validation key to be output.

When the unencrypted digital contents are received, microcomputer 320 replays and outputs the digital contents without decrypting them.

Decoder 350 decodes the digital contents output from microcomputer 320 to output audio signal. Decoder 350 is preferred to be MPEG decoder.

Fig. 23 is a flow chart illustrating the method of decrypting the encrypted digital contents in case the encrypted digital contents are input from PC to the replaying de-

vice constructed as in Fig. 22 .

Microcomputer 320 determines whether the key information is input from PC (S510) and stores the input key information in memory 300 when the key information is determined to be input (S515).

After storing the key information in memory 300, microcomputer 320 determines whether the encrypted digital contents are input from PC (S520). When the encrypted digital contents are determined to be input at the step of S520, microcomputer 320 stores the digital contents in memory 300 and then reads the header from the digital contents according to the decryption algorithm stored in memory 300 after the transmission process is completed (S525). When the encrypted digital contents are determined not to be input, they are recognized as an error (S580) and the decryption process is terminated.

Next, microcomputer 320 determines whether the copyright support code exists in the header of the read digital contents (S530).

If the copyright support code is determined to exist, the digital contents are recognized to be protected by copyright and the read unencrypted header information is stored at memory 300 as a predetermined variable (S535).

When the digital contents is determined to be protected by copyright, microcomputer 320 generates the user key using the key information and the key generation algorithm. Microcomputer 320 calculates a hash value of the generated user key by hash algorithm stored in memory 300 (S540).

Next, microcomputer 320 determines whether the calculated hash value of the user key is identical with a hash value of the user key in the user authorization information of the header (S545).

When the calculated hash value of the user key is determined to coincide with the hash value of the user key in the header, the user is recognized to be authorized and the temporary validation key is decrypted using the user key (S550). The encrypted header is decrypted using the decrypted temporary validation key (S555).

At the determination step of S545, a message of "Not authorized" is output and the decryption process is terminated when the calculated hash value of the user key is

determined not to be identical with the hash value of the user key in the header.

It is determined according to hash value of the entire header whether the entire header is changed in order to determine whether the user is authorized to decrypts and replay the digital contents (S455). The hash value is calculated by applying the entire header to hash algorithm (S560).

The change of the entire header is determined according to whether the hash value of the entire header calculated at the step of S560 is identical with a hash value of the entire header stored in the header (S565).

In case the header is determined not to be changed, that is, the hash value of the entire header calculated at the step of S560 is identical with the hash value of the entire header stored in the header, the encrypted digital contents are decrypted (S570). The additional information is processed and then replayed in case the additional information does not exist (S575).

When the header is determined to be changed at the step of S565, that is, the calculated hash value of the entire header is not identical with the hash value of the entire header stored in the header, the user is recognized not to be authorized so that the decryption process is terminated for the user not to replay the digital contents (S585).

In the present invention, the supplied encrypt digital content cannot be replayed without the supply of the decoding algorithm and the key information. Therefore, when the digital content is illegally copied, it cannot be replayed, preventing illegal copy and unauthorized distribution. This will prevent significant loses for the provider of the digital content caused by illegal copying and unauthorized distribution while forcing the user to acquire the digital content via a legitimate route.

While this invention has been described in connection with what is presently considered to be the most practical and preferred embodiment, it is to be understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

What is claimed is:

1. A digital content encryption apparatus of the digital content transmission system comprising:

a terminal unit having decryption algorithm, said terminal unit transmitting identity characters of a user and receiving and storing key information, said terminal unit receiving protocol including encrypted digital contents requested by the user and decrypting copyright protection protocol using the decryption algorithm and the key information to replay the digital contents, said key information formed to correspond to the identity characters; and

a service server having encryption algorithm, said service server generating the key information corresponding to the identity characters transmitted from the terminal unit and transmitting the key information to the terminal unit, said service server encrypting the digital contents using the key information and the encryption algorithm, said terminal unit transmitting to the copyright protection protocol to the terminal unit, said copyright protection protocol having a header and being formed by adding the encrypted digital contents to the header.

2. The apparatus of claim 1, wherein the terminal unit further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key being decrypted by the user key, said encrypted digital contents included in the copyright protection protocol being decrypted by the temporary validation key.

3. The apparatus of claim 1, wherein the terminal unit comprises:

a first interface receiving the key information;

a use authority identifier identifying whether the user is authorized by comparing a hash value of the user key with a hash value set in user authorization information after reading the user authorization information of the header from the copyright protection protocol, the use authority identifier generating the user key by using the key

information;

a temporary validation key decryptor decrypting the temporary validation key using the user key; and

a digital content decryptor decrypting the encrypted digital contents using the temporary validation key decrypted by the temporary validation key decryptor.

4. The apparatus of claim 1, wherein the service server further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key generated in response to the user's request being decrypted by the user key, said encrypted digital contents being decrypted by the temporary validation key.

5. The apparatus of claim 1, wherein said service server comprises:

a second interface receiving the identity characters input from the terminal unit;

key information generator generating the key information corresponding to the identity characters input from the second interface;

a user key generator generating the user key using the key information generated by the key information generator;

a temporary validation key generator generating the temporary validation key when the user accesses the service server through the second interface;

a user authorization information generator encrypting the temporary validation key using the user key generated by the user key generator to generate user authorization information;

a header generator generating the header using the user key, said header including the user authorization information; and

a protocol format generator generates the copyright protection protocol by adding the encrypted digital contents to the header generated by the header generator.

6. The apparatus of claim 1, further comprising:

a service sanction agent server receiving from the service server a signal con-

cerning digital content fees, said digital content fees caused by the transmission of the digital content requested by the user, said signal accumulating the digital content fees for the registered user's ID.

7. The apparatus of claim 1, wherein the terminal unit is connected to a public switched telephone network, said terminal unit having a network access program.

8. The apparatus of claim 1, wherein the terminal unit connected to a network, said terminal unit having a network access program.

9. The apparatus of claim 1, wherein the terminal unit is connected to a wireless network, said terminal unit having a network access program.

10. A digital content encryption apparatus of the digital content transmission system comprising:

a terminal unit having decryption algorithm, said terminal unit transmitting identity characters of a user and receiving and storing key information, said terminal unit receiving protocol including encrypted digital contents requested by the user and decrypting copyright protection protocol using the decryption algorithm and the key information to replay the digital contents, said key information formed to correspond to the identity characters;

a service server having encryption algorithm, said service server transmitting the key information to the terminal unit, said service server encrypting the digital contents using the key information and the encryption algorithm, said terminal unit transmitting to the copyright protection protocol to the terminal unit, said copyright protection protocol having a header and being formed by adding the encrypted digital contents to the header; and

a host server generating the key information corresponding to the identity characters transmitted from the service server and transmitting the key information to the service server, said host server storing the key information with the identity characters.

11. The apparatus of claim 10, wherein the terminal unit further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key being decrypted by the user key, said encrypted digital contents included in the copyright protection protocol being decrypted by the temporary validation key.

12. The apparatus of claim 10, wherein the terminal unit comprises:

a first interface receiving the key information;

a use authority identifier identifying whether the user is authorized by comparing a hash value of the user key with a hash value set in user authorization information after reading the user authorization information of the header from the copyright protection protocol, the use authority identifier generating the user key by using the key information;

a temporary validation key decryptor decrypting the temporary validation key using the user key; and

a digital content decryptor decrypting the encrypted digital contents using the temporary validation key decrypted by the temporary validation key decryptor.

13. The apparatus of claim 10, wherein the service server further comprises a user key and a temporary validation key, said user key being generated by the key information and key generation algorithm, said temporary validation key generated in response to the user's request being decrypted by the user key, said encrypted digital contents being decrypted by the temporary validation key.

14. The apparatus of claim 10, wherein said service server comprises:

a second interface receiving the identity characters input from the terminal unit;

a user key generator generating the user key using the key information;

a temporary validation key generator generating the temporary validation key when the user accesses the service server through the second interface;

a user authorization information generator encrypting the temporary validation key using the user key generated by the user key generator to generate user authorization information;

a header generator generating the header using the user key, said header including the user authorization information; and

a protocol format generator generates the copyright protection protocol by adding the encrypted digital contents to the header generated by the header generator.

15. The apparatus of claim 10, wherein said host server comprises:

key information generator generating the key information corresponding to the identity characters input from the second interface.

16. The apparatus of claim 10, further comprising:

a service sanction agent server receiving from the service server a signal concerning digital content fees, said digital content fees caused by the transmission of the digital content requested by the user, said signal accumulating the digital content fees for the registered user's ID.

17. The apparatus of claim 10, wherein the terminal unit is connected to a public switched telephone network, said terminal unit having a network access program.

18. The apparatus of claim 10, wherein the terminal unit connected to a network, said terminal unit having a network access program.

19. The apparatus of claim 10, wherein the terminal unit is connected to a wireless network, said terminal unit having a network access program.

20. A digital content encryption apparatus of the digital content transmission system comprising:

a protocol format generator generating a copyright protection protocol, said

copyright protection protocol including a header and digital contents, said digital contents being encrypted, said header having information for decrypting and explaining the digital contents; and

a protocol format decoder having decryption algorithm, said protocol format decoder decrypting and replaying the digital contents according to the information of the header received from the protocol format generator.

21. The apparatus of claim 20, wherein the protocol format generator generates a user key by adding key information to key generation algorithm and calculates a hash value by adding the user key to hash algorithm, said protocol format generator encrypting a temporary validation key by using the user key, said header including user authorization information with the hash value and the encrypted temporary validation key, said key information being formed to correspond to identity characters of a user.

22. The apparatus of claim 20, wherein the protocol format decoder generates a user key by adding key information to key generation algorithm and decrypts a temporary validation key by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, said key information being formed to correspond to identity characters of a user.

23. A digital content encryption apparatus of the digital content transmission system comprising a protocol format decoder for copyright protection, said protocol format decoder having decryption algorithm and receiving copyright protection protocol including encrypted digital contents, said protocol format decoder decrypting the copyright protection protocol using the decryption algorithm and key information to replay the encrypted digital contents.

24. The apparatus of claim 23, wherein the protocol format decoder generates a user key by adding key information to key generation algorithm and decrypts a temporary validation key from user authorization information by using the user key, said protocol for-

mat decoder decrypting the encrypted digital contents with the temporary validation key, said user authorization information being included in the copyright protection protocol.

25. A protocol for protecting copyright of digital contents including a header and the digital contents, said digital contents being encrypted, said header having information for decrypting the digital contents.

26. The protocol of claim 25, further comprising a field for indicating the size of the encrypted digital contents, and an additional information field.

27. The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, and an encrypted header field.

28. The protocol of claim 25, wherein the header comprises a copyright support field for indicating whether the digital contents are under copyright protection, an unencrypted header field, a field for indicating the size of the unencrypted header field, an encrypted header field, a field for indicating the size of the encrypted header field.

29. The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating user authorization information at PC, and a field for indicating user authorization information at a replaying device.

30. The protocol of claim 29, wherein the field for indicating user authorization information at the PC and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of the user key, and a field for indicating the size of the hash value generated by hash algorithm, a field for indi-

cating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

31. The protocol of claim 27 or 28, wherein the unencrypted header field comprises a copyright library version field, a digital content conversion format field, a field for indicating the code of a digital content provider, a key generation algorithm field, a digital content encryption algorithm field, a field for indicating the number of users sharing PC, a field for indicating the number of users sharing a replaying device, a field for indicating user authorization information at the PC, and a field for indicating user authorization information at the replaying device.

32. The protocol of claim 31, wherein the field for indicating user authorization information at the PC and the field for indicating user authorization information at the replaying device comprise a field for indicating a hash value of the user key, and a field for indicating the size of the hash value generated by hash algorithm, a field for indicating a resultant value of an encrypted temporary validation key, and a field for indicating the size of the resultant value of the encrypted temporary validation key, respectively.

33. The protocol format of claim 27 or 28, wherein the encrypted header field comprises a field for encryption algorithm of the digital content, a field for indicating a basic process unit of the digital content, a field for indicating the number of encrypted byte, and a hash value field for a hash value for determining the state of the entire header.

34. A digital content encryption method of the digital content transmission system comprising the steps of:

a user inputting identity characters for membership registration through a terminal unit;

determining whether the user is registered by checking the input identity char-

acters;

storing information on the membership registration when the user is determined to be unregistered;

transmitting key information to the user in response to the user's request for digital contents;

determining whether a request signal for downloading digital contents;

encrypting the digital contents by a temporary validation key when the request signal is determined to be input from the user; and

transmitting the digital contents.

35. The method of claim 34 further comprising the step of transmitting information on the service fee to a service sanction agent server, said the information on the service fee being generated when the digital contents is transmitted to the user.

36. A method for generating user authorization information of digital contents comprising the steps of:

determining whether identity characters are received from a service server;

comparing the received identity characters with stored identity characters to determine whether identical identity characters with the received identity characters exist among the stored identity characters when the identity characters are received;

generating the key information when identical identity characters with the received identity characters is determined not to exist;

transmitting key information to the service server in response to the request of the service server; and

storing the user's identity characters with the transmitted key information.

37. A digital content encryption method of the digital content transmission system comprising the steps of:

receiving a request signal for digital contents from a user;

generating user authorization information using internally stored data when the

request signal is received;

generating a header having information on the digital contents and the user authorization information;

encrypting the digital contents; and

transmitting copyright protection protocol generated by adding the encrypted digital contents to the header.

38. The method of claim 37, wherein the internally stored data is key information generated correspondingly to the user's identity characters.

39. The method of claim 37, wherein the step of generating user authorization information further comprises:

generating a temporary validation key in response to the received request signal for the digital contents;

generating a user key using a key information; and

generating the encrypted user authorization information using the temporary validation key and the user key.

40. The method of claim 39, wherein the user authorization information comprises the encrypted temporary validation key and a hash value of the user key.

41. A method for encrypting digital content communication protocol comprising the steps of:

generating a temporary validation key when a user's request for the digital contents exists;

determining whether digital content encryption algorithm defined by a digital content provider exists;

generating a header according to the digital content encryption algorithm when the digital content encryption algorithm defined by the provider exists, and generating a header according to a basic algorithm when the digital content encryption algorithm de-

fined by the provider does not exist;

encrypting the digital contents after generating the header; and

adding the generated header to a front end of the digital contents.

42. The method of claim 41, further comprising the steps of:

determining whether additional information exists;

generating an additional information field when the additional information is determined to exist; and

adding the additional information field to a rear end of the digital contents.

43. The method of claim 41, wherein the step of generating the header comprises the step of:

generating copyright support information field and a field for indicating the size of an unencrypted header information and then adding them to the header;

adding the unencrypted header information field to the header;

generating user authorization information using a key information;

adding the generated user authorization information to the header;

generating header information for encrypting the digital contents;

encrypting the generated header information; and

adding an encrypted header information field and a field for indicating the size of the encrypted header information to the header.

44. The method of claim 43, wherein the step for generating the user authorization information comprises:

determining the existence of the key information or the temporary validation key;

using the key information to generate the user key when the key information and the temporary validation key are determined to exist;

calculating a hash value of the generated user key; and

encrypting the temporary validation key using the key encryption algorithm

and the generated user key after calculating the hash value.

45. A method for decrypting an encrypted digital contents comprising the steps of:

transmitting a digital content request signal to a service server;

receiving data and copyright protection protocol from the service server;

generating calculated data using internally stored data from the received data;

comparing the calculated data with data set in user authorization information included in the copyright protection protocol; and

confirming the use authority to decrypt the encrypted digital contents when the calculated data coincides with the data set in the user authorization information.

46. The method of claim 45, further comprising the step of decrypting and replaying the encrypted digital contents.

47. The method of claim 45, wherein the internally stored data are key information generated correspondingly to the user's identity characters.

48. The method of claim 45, wherein the user authorization information comprises a hash value of a user key generated by key information and an encrypted temporary validation key.

49. The method of claim 45, wherein the data set in the user authorization information is a hash value of a user key generated by key information.

50. The method of claim 45, wherein the calculated data are calculated by applying key information to key generation algorithm, a hash value being calculated from the calculated by hash algorithm, said calculated hash value being determined whether it is identical to a hash value set in the user authorization information, a temporary validation key included in the user authorization information being decrypted when said calculated hash value is determined to be identical to the set hash value, an encrypted header in-

cluded in the copyright protection protocol being decrypted the decrypted temporary validation key, said encrypted header being calculated into a hash value of a header using the hash algorithm, said key information being formed to corresponding to the user's identity characters.

51. The method of claim 50, wherein the calculated hash value of the header is determined whether it is identical to the hash value of a header set in the header, said encrypted temporary validation key being decrypted using the calculated data when the calculated hash value of the header is identical with the set header value of the header to confirm the use authority, said temporary validation key being replayed while decrypting the encrypted digital contents.

52. A method for receiving key information for user to be authorized to receive digital contents from a service server, comprising the steps of:

opening a screen for providing the digital contents via telecommunication;

requesting membership registration through the opened screen;

receiving key information corresponding to the membership registration; and

storing the received key information.

53. The method of claim 52, wherein the received key information is transmitted to an external slave device to be stored.

54. A method for receiving key information for user to be authorized to receive digital contents from a service server, comprising the steps of:

a processor opening a screen for providing the digital contents when a user inputs a key signal via an input device;

inputting request data on the open screen and transmitting it via the service server;

receiving the key information corresponding to the transmitted request data; and

storing the received key information.

55. The method of claim 54, wherein the request data are the user's identity characters.

56. The method of claim 54, wherein the key information received in the step of receiving the key information is transmitted to an external slave device to be stored.

57. A replaying device with decrypting function, comprising:

a memory storing an algorithm for decrypting protocol including encrypted digital contents, said memory further storing key information received when a user is a new member and the protocol received when the digital contents are requested;

a microcomputer storing the protocol inputted from an external device in the memory, and controlling output and encryption of the protocol according to the algorithm stored in the memory in accordance with a key signal received through a user key input unit; and

a decoder decoding the digital contents outputted from the microcomputer.

58. The replaying device of claim 57, wherein the decoder is a MPEG decoder.

59. The replaying device of claim 57, wherein the memory is a flash memory.

60. The replaying device of claim 57, wherein the microcomputer generates the user key through user authorization information of a received header by using the key information stored in the memory when the digital contents inputted according to the stored algorithm are encrypted, said microcomputer decrypting a temporary validation key included in the user authorization information of the header using the generated user key, said microcomputer decrypting and outputting the encrypted digital contents using a decrypted temporary validation key.

61. The replaying device of claim 57, wherein the microcomputer replays and outputs

the digital contents without decrypting them when the received digital contents are un-encrypted.

62. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving protocol comprising a header and encrypted digital contents, said header including user authorization information; and

storing the protocol in a record medium.

63. The method of claim 62, further comprising the step of decrypting and replaying the encrypted digital contents stored in the record media.

64. The method of claim 62, wherein the user authorization information comprises a hash value of a user key and an encrypted temporary validation key, said user key being generated by key information.

65. The method of claim 62, wherein the record medium is a flash memory.

66. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving encrypted digital contents and a header, said header having user authorization information;

generating calculated data using internally stored data after receiving the digital contents;

comparing the calculated data with the user authorization information;

decrypting the encrypted digital contents when the calculated data and the user authorization information are determined to be identical; and

replaying the decrypted digital contents.

67. The method of claim 66, wherein the calculated data are calculated by applying key

information to key generation algorithm,

a hash value being calculated from the calculated by hash algorithm,

said calculated hash value being determined whether it is identical to a hash value set in the user authorization information,

a temporary validation key included in the user authorization information being decrypted when said calculated hash value is determined to be identical to the set hash value,

an encrypted header included in the copyright protection protocol being decrypted the decrypted temporary validation key,

said encrypted header being calculated into a hash value of a header using the hash algorithm,

said key information being formed to corresponding to the user's identity characters,

said calculated hash value of the header being determined whether it is identical to the hash value of a header set in the header,

said encrypted temporary validation key being decrypted using the calculated data when the calculated hash value of the header is identical with the set header value of the header to confirm the use authority,

said temporary validation key being replayed while decrypting the encrypted digital contents.

68. The method of claim 66, wherein the internally stored data are key information generated correspondingly to user's identity characters.

69. A digital content decrypting method of a replaying device with decrypting function, comprising the steps of:

receiving key information and storing it on a record medium;

receiving encrypted digital contents and a header, said header having user authorization information;

generating a user key using the key information;

comparing a hash value of a user key set in the received user authorization information and a hash value of the generated user key; and

decrypting the encrypted digital contents when the hash value of the generated user key and the hash value of a user key set in the received user authorization information data are determined to be identical.

Abstract

A digital content encryption apparatus and method thereof encrypts and transmits the digital content from the digital content transmission system by using the key informtion, the user key and the temporary validation key, to decrypt and replay the encryted digital content in the user terminal by using the key information and the user authorization information.

The registered user is provided with a unique key information. The user key is generated by applying the key information to the key generation algorithm and the temporary validation key generated when the registered user accesses the server is encrypted by the user key. The digital contents are encryted by using the temporary validation key. The decryption algorithm gets the user to decrypt and replay the encrypted digital content by receiving the key information which corresponds one-to-one to the identity characters.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

En-Seong Kang, et al.

Serial No.:	*To Be Assigned*	Examiner:	*To Be Assigned*
Filed:	December 22, 1998	Art Unit:	*To Be Assigned*

For: THE DIGITAL CONTENT ENCRYPTION APPARATUS AND METHOD THEREOF

TRANSMITTAL OF DECLARATION

The Assistant Commissioner
of Patents
Washington, D.C. 20231

Sir:

Accompanying this transmittal is a Declaration for the above-referenced application.

Respectfully submitted,

Robert E. Bushnell
Reg. No.: 27,774
Attorney for the Applicant

1522 K Street, N.W.
Suite 300
Washington, D.C. 20005-1202
Telephone: (202) 638-5740
Telefacsimile: (202) 628-0755

Folio: P55501
Date: 12/22/98
I.D.: REB/lj

FIG. 1

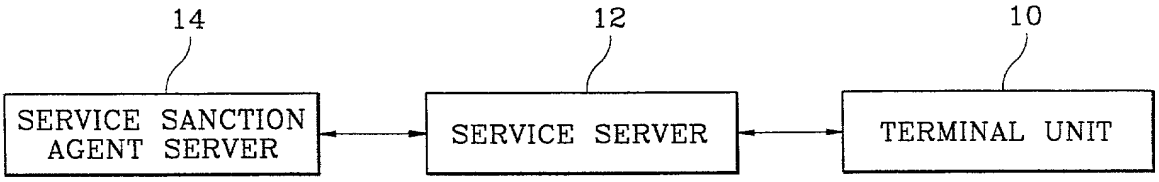

14
12
10
SERVICE SANCTION AGENT SERVER
SERVICE SERVER
TERMINAL UNIT

FIG. 2

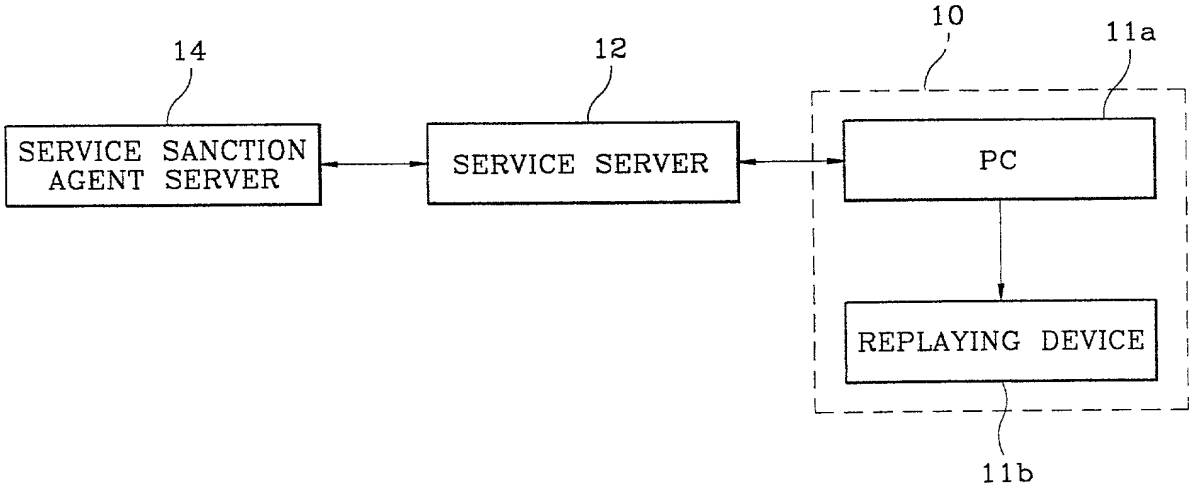

14
12
10
11a
SERVICE SANCTION AGENT SERVER
SERVICE SERVER
PC
REPLAYING DEVICE
11b

FIG. 3

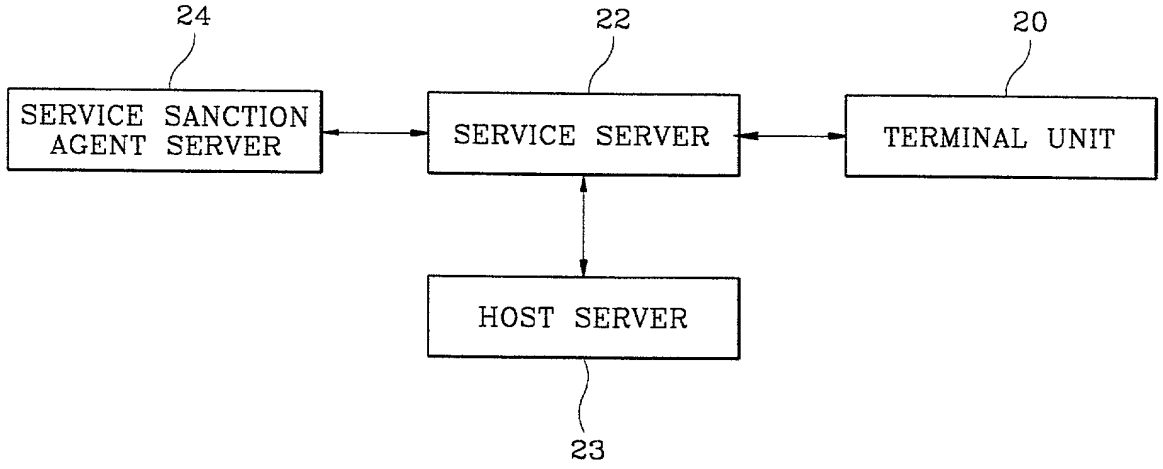

24
22
20
SERVICE SANCTION AGENT SERVER
SERVICE SERVER
TERMINAL UNIT
HOST SERVER
23

FIG. 4

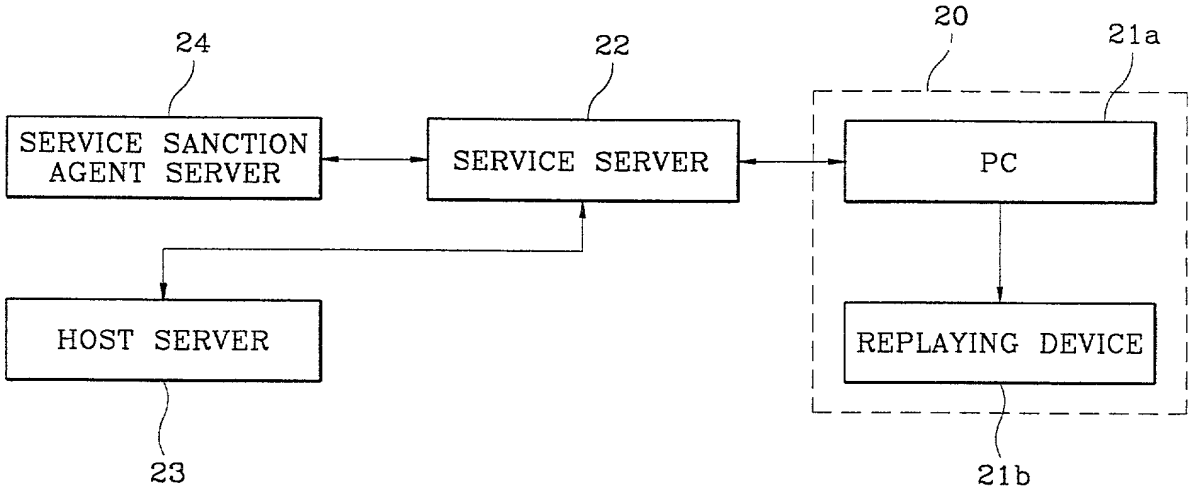

20
21a
24
22
SERVICE SANCTION AGENT SERVER
SERVICE SERVER
PC
HOST SERVER
REPLAYING DEVICE
23
21b

FIG. 5

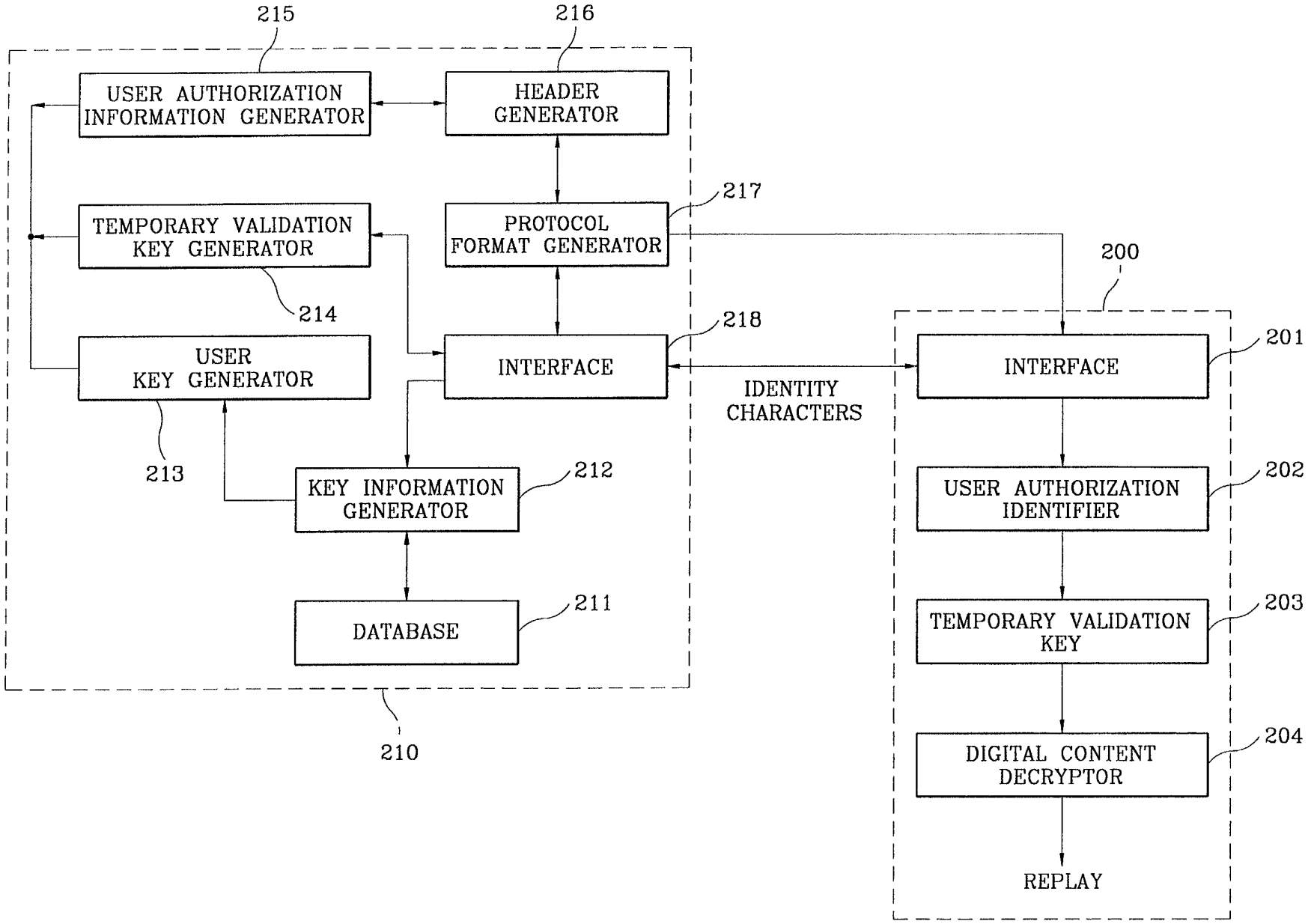


FIG. 6

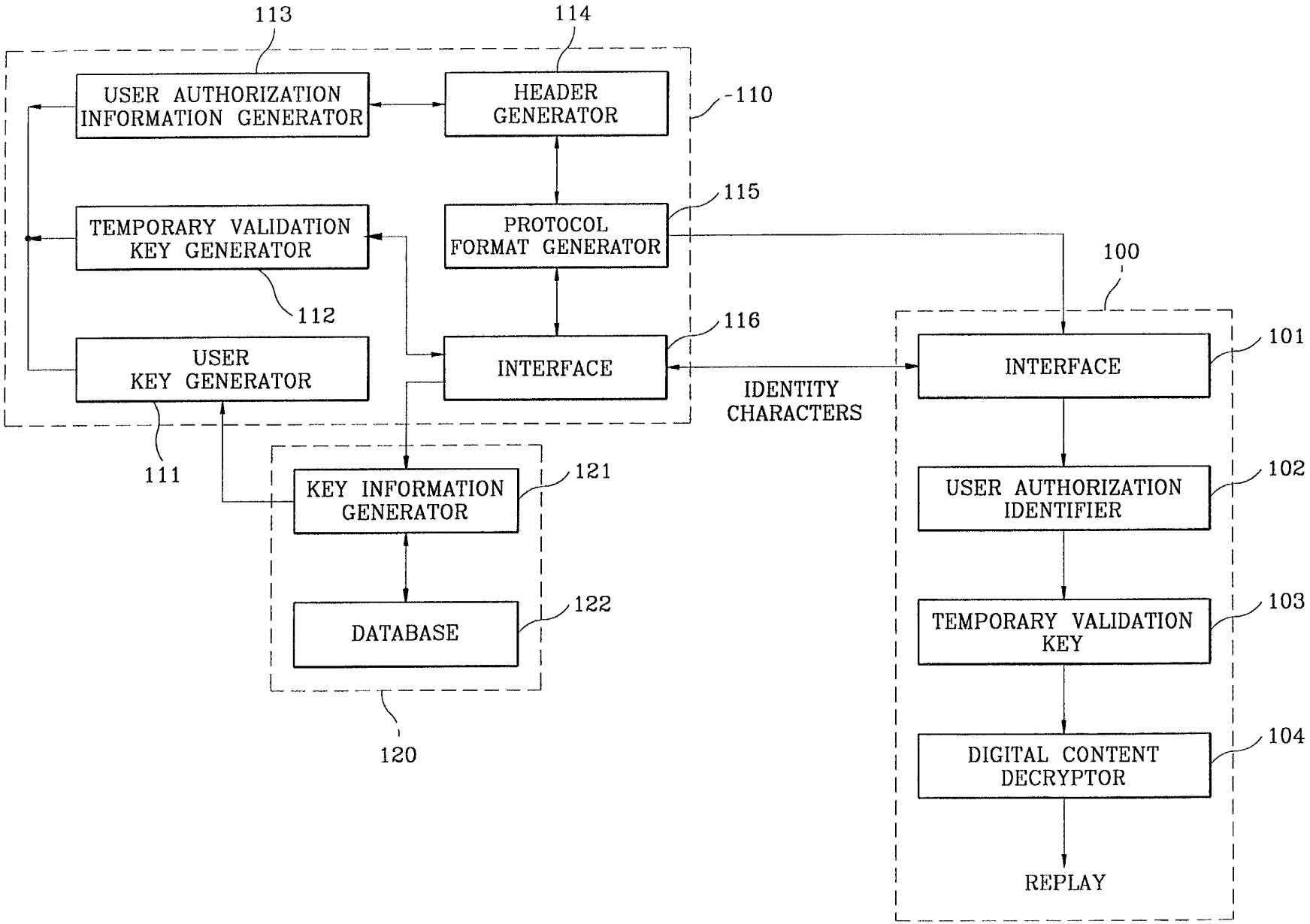


FIG. 7

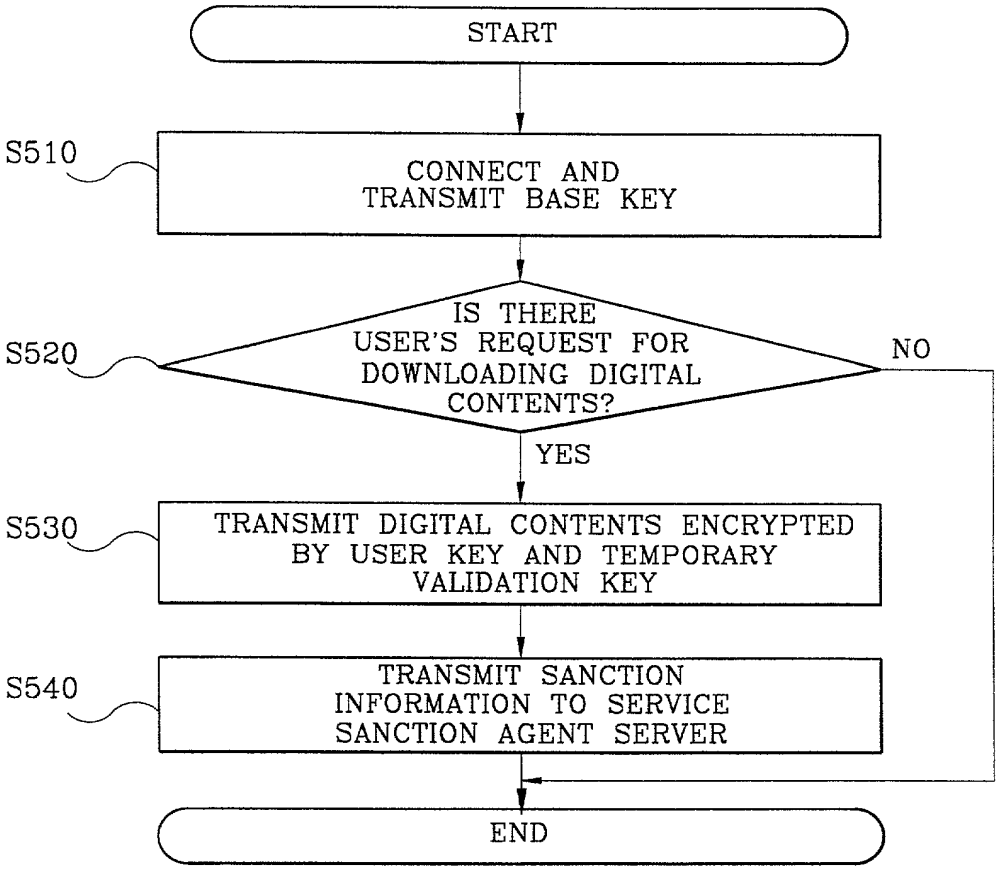

START
S510
CONNECT AND TRANSMIT BASE KEY
S520
IS THERE USER'S REQUEST FOR DOWNLOADING DIGITAL CONTENTS?
NO
YES
S530
TRANSMIT DIGITAL CONTENTS ENCRYPTED BY USER KEY AND TEMPORARY VALIDATION KEY
S540
TRANSMIT SANCTION INFORMATION TO SERVICE SANCTION AGENT SERVER
END

FIG. 8

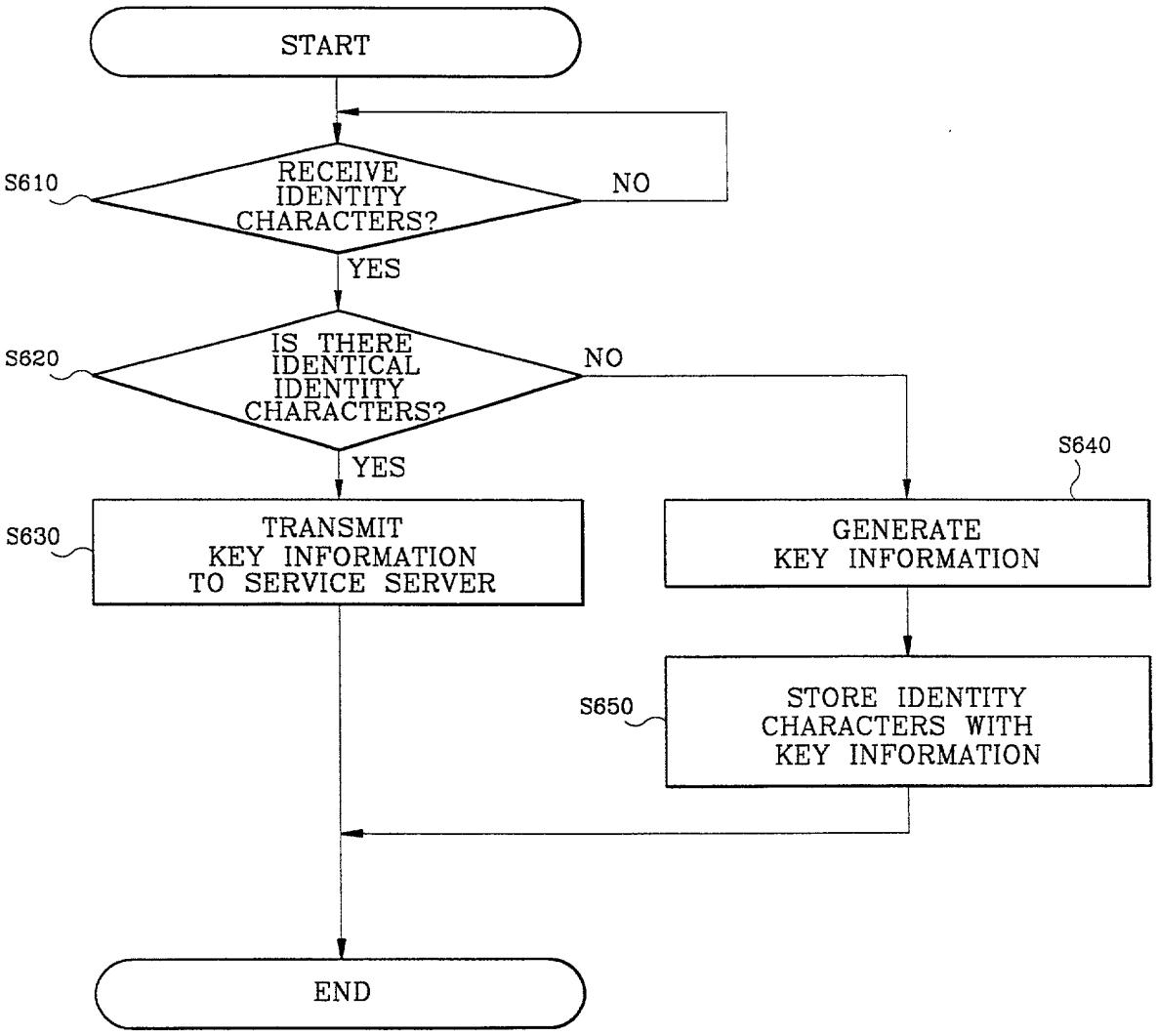

START
S610
RECEIVE IDENTITY CHARACTERS?
NO
YES
S620
IS THERE IDENTICAL IDENTITY CHARACTERS?
NO
YES
S630
TRANSMIT KEY INFORMATION TO SERVICE SERVER
S640
GENERATE KEY INFORMATION
S650
STORE IDENTITY CHARACTERS WITH KEY INFORMATION
END

FIG. 9

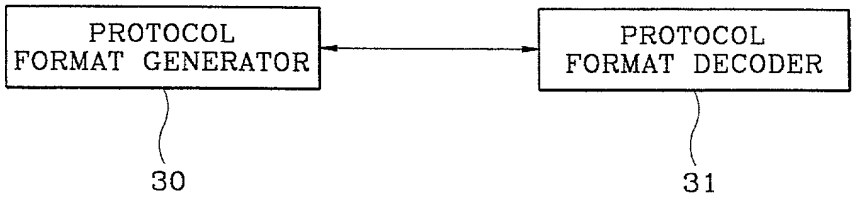


FIG. 10

HEADER	ENCRYPTED DIGITAL CONTENTS

FIG. 11

HEADER	SIZE OF ENCRYPTED DIGITAL CONTENTS	ENCRYPTED DIGITAL CONTENTS	ADDITIONAL INFORMATION

FIG. 12

COPYRIGHT SUPPORT INFORMATION	UNENCRYPTED HEADER	ENCRYPTED HEADER

FIG. 13

COPYRIGHT SUPPORT INFORMATION	OFFSET	SIZE OF UNENCRYPTED HEADER	UNENCRYPTED HEADER	SIZE OF ENCRYPTED HEADER	ENCRYPTED HEADER	ADDITIONAL INFORMATION

FIG. 14

COPYRIGHT LIBRARY VERSION	INFORMATION ON DIGITAL CONTENT CONVERSION FORMAT	KEY GENERATION ALGORITHM	DIGITAL CONTENT ENCRYPTION ALGORITHM	USER AUTHORIZATION INFORMATION AT PC	USER AUTHORIZTION INFORMATION AT REPLAYING DEVICE

FIG. 15

COPYRIGHT LIBRARY VERSION	DIGITAL CONTENT CONVERSION FORMAT	DIGITAL CONTENT PROVIDER CODE	KEY GENERATION ALGORITHM	DIGITAL CONTENT ENCRYPTION ALGORITHM	NUMBER OF USERS SHARING PC	NUMBER OF USERS SHARING REPLAYING DEVICE	USER AUTHORIZATION INFORMATION AT PC	USER AUTHORIZTION INFORMATION AT REPLAYING DEVICE

FIG. 16

SIZE OF HASH VALUE	HASH VALUE	SIZE OF RESULTANT VALUE OF ENCRYPTED TEMPORARY VALIDATION KEY	RESULTANT VALUE OF ENCRYPTED TEMPORARY VALIDATION KEY

FIG. 17

BASIC PROCESS UNIT OF DIGITAL CONTENT	ENCRYPTION SIZE	ENCRYPTED FRAME UNIT	HASH VALUE FOR DETERMINING THE STATE OF HEADER

FIG. 18

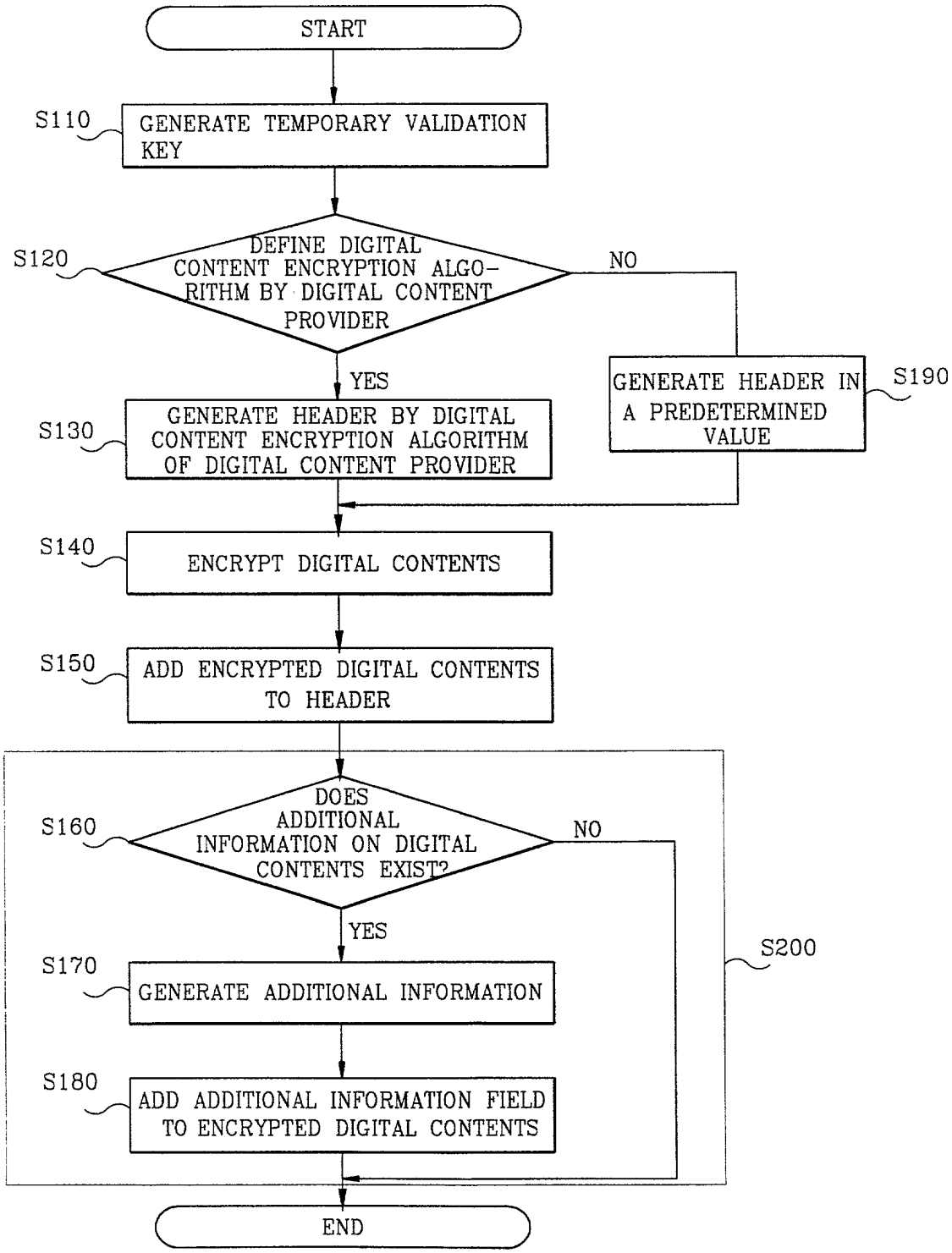

START
S110
GENERATE TEMPORARY VALIDATION KEY
S120
DEFINE DIGITAL CONTENT ENCRYPTION ALGORITHM BY DIGITAL CONTENT PROVIDER
NO
YES
S130
GENERATE HEADER BY DIGITAL CONTENT ENCRYPTION ALGORITHM OF DIGITAL CONTENT PROVIDER
GENERATE HEADER IN A PREDETERMINED VALUE
S190
S140
ENCRYPT DIGITAL CONTENTS
S150
ADD ENCRYPTED DIGITAL CONTENTS TO HEADER
S160
DOES ADDITIONAL INFORMATION ON DIGITAL CONTENTS EXIST?
NO
YES
S170
GENERATE ADDITIONAL INFORMATION
S180
ADD ADDITIONAL INFORMATION FIELD TO ENCRYPTED DIGITAL CONTENTS
S200
END

FIG. 19

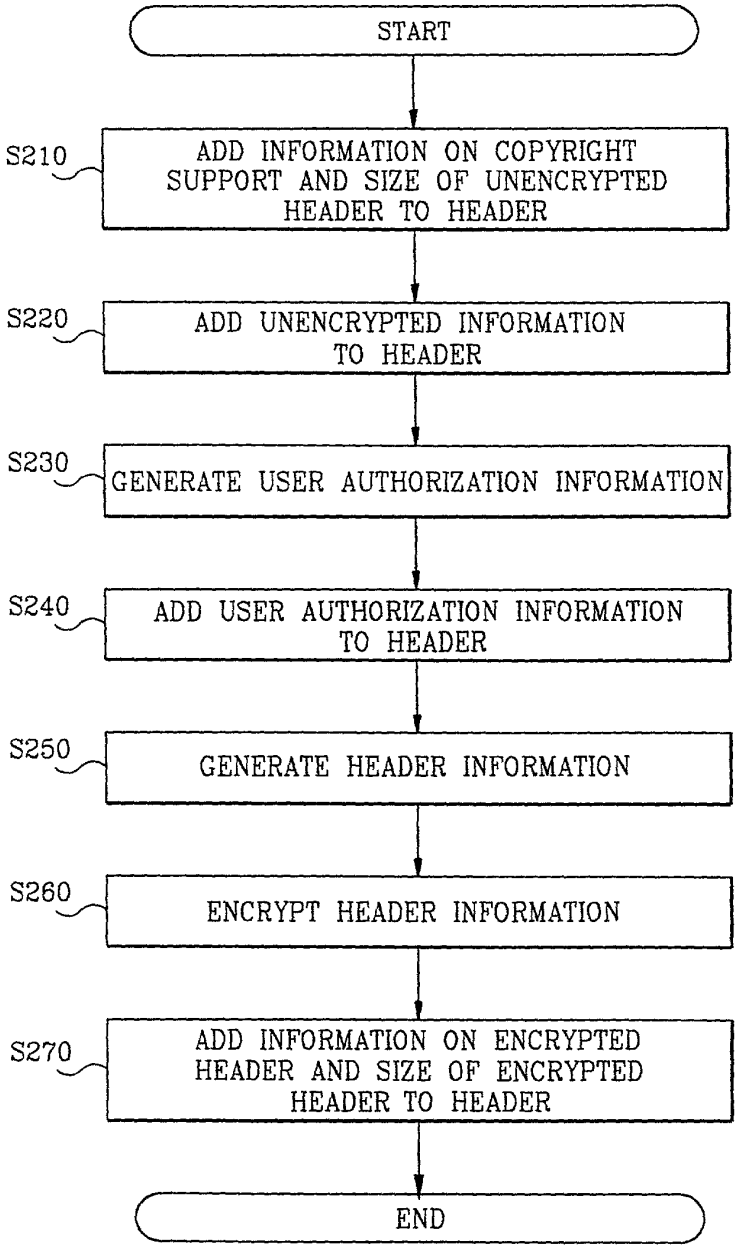

START
S210
ADD INFORMATION ON COPYRIGHT SUPPORT AND SIZE OF UNENCRYPTED HEADER TO HEADER
S220
ADD UNENCRYPTED INFORMATION TO HEADER
S230
GENERATE USER AUTHORIZATION INFORMATION
S240
ADD USER AUTHORIZATION INFORMATION TO HEADER
S250
GENERATE HEADER INFORMATION
S260
ENCRYPT HEADER INFORMATION
S270
ADD INFORMATION ON ENCRYPTED HEADER AND SIZE OF ENCRYPTED HEADER TO HEADER
END

FIG. 20

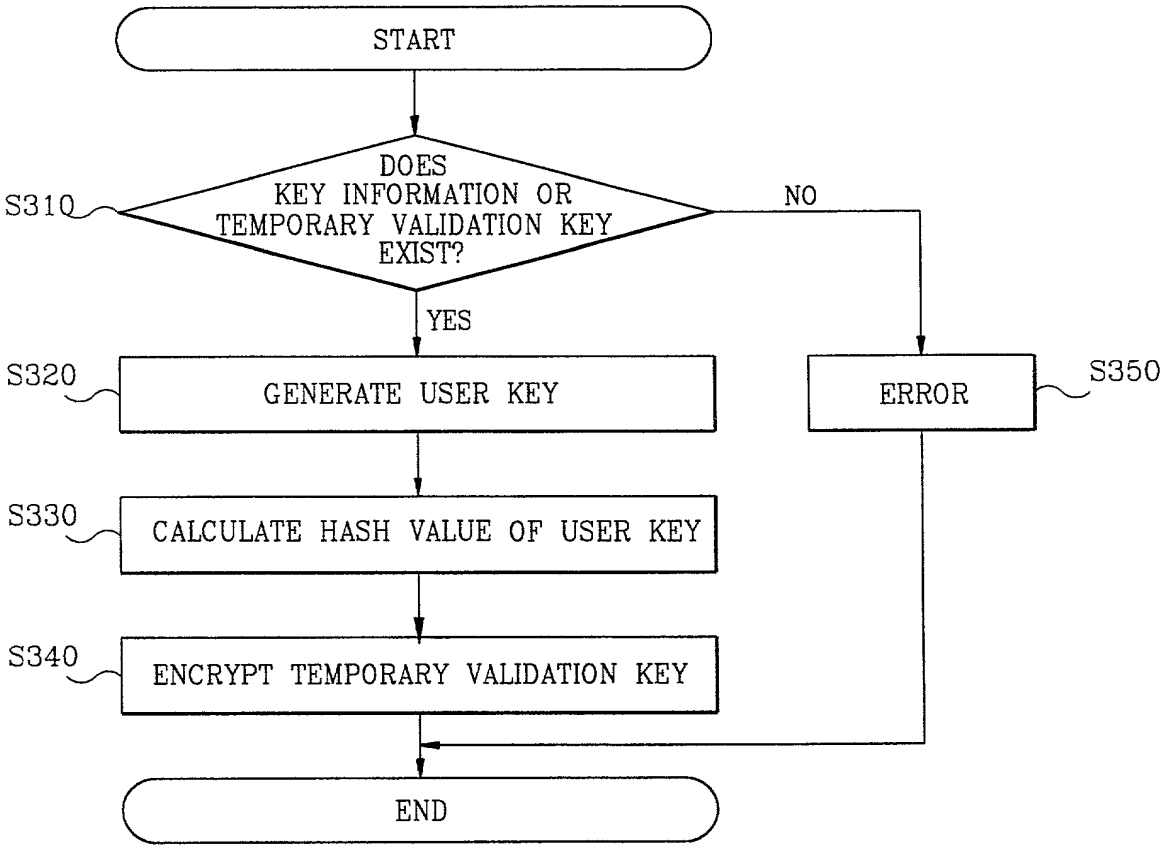

START
DOES KEY INFORMATION OR TEMPORARY VALIDATION KEY EXIST?
S310
NO
YES
S320
GENERATE USER KEY
S330
CALCULATE HASH VALUE OF USER KEY
S340
ENCRYPT TEMPORARY VALIDATION KEY
ERROR
S350
END

FIG. 21A

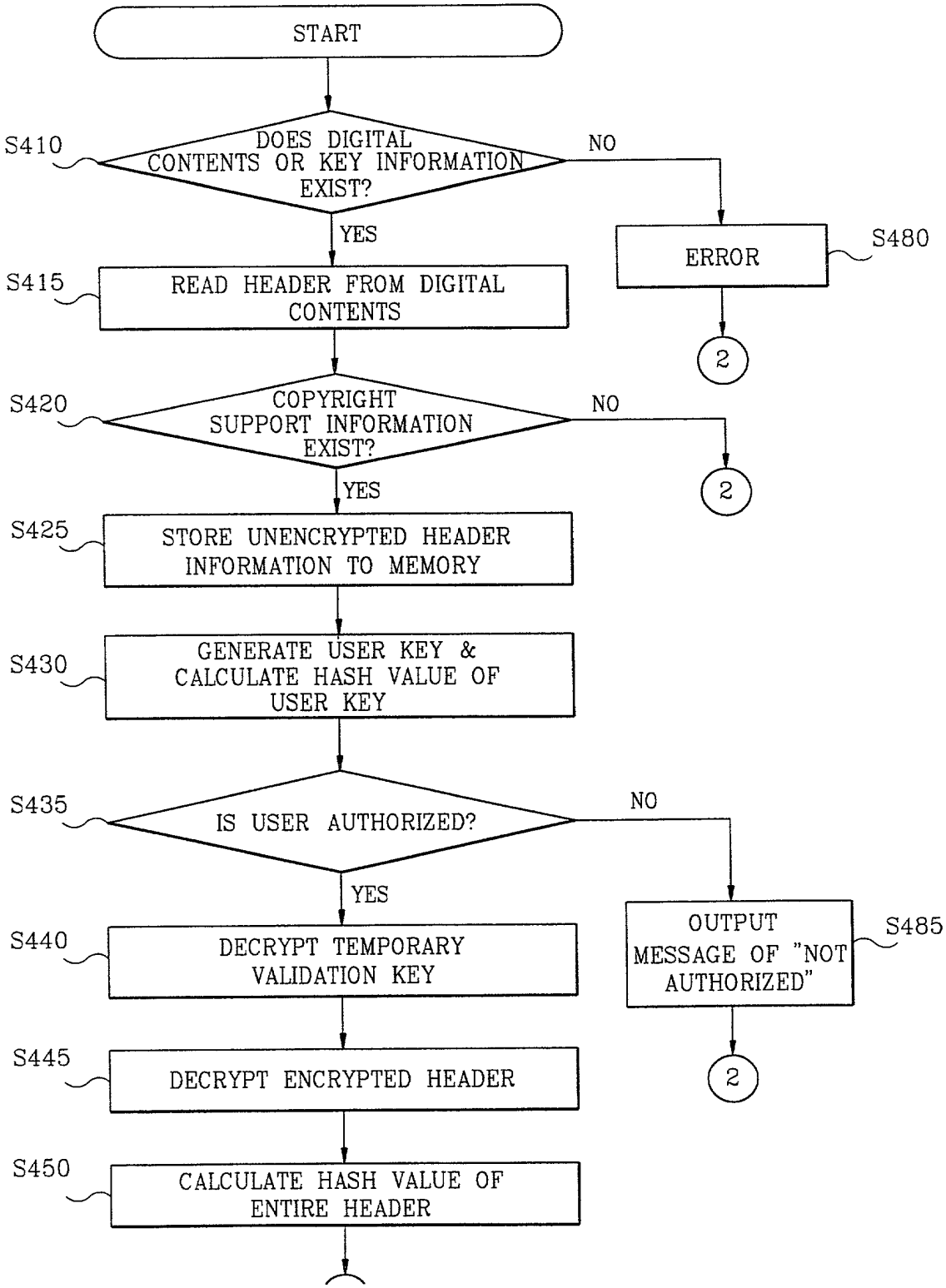

START
S410
DOES DIGITAL CONTENTS OR KEY INFORMATION EXIST?
NO
YES
ERROR
S480
S415
READ HEADER FROM DIGITAL CONTENTS
2
S420
COPYRIGHT SUPPORT INFORMATION EXIST?
NO
YES
2
S425
STORE UNENCRYPTED HEADER INFORMATION TO MEMORY
S430
GENERATE USER KEY & CALCULATE HASH VALUE OF USER KEY
S435
IS USER AUTHORIZED?
NO
YES
OUTPUT MESSAGE OF "NOT AUTHORIZED"
S485
2
S440
DECRYPT TEMPORARY VALIDATION KEY
S445
DECRYPT ENCRYPTED HEADER
S450
CALCULATE HASH VALUE OF ENTIRE HEADER

FIG. 21B

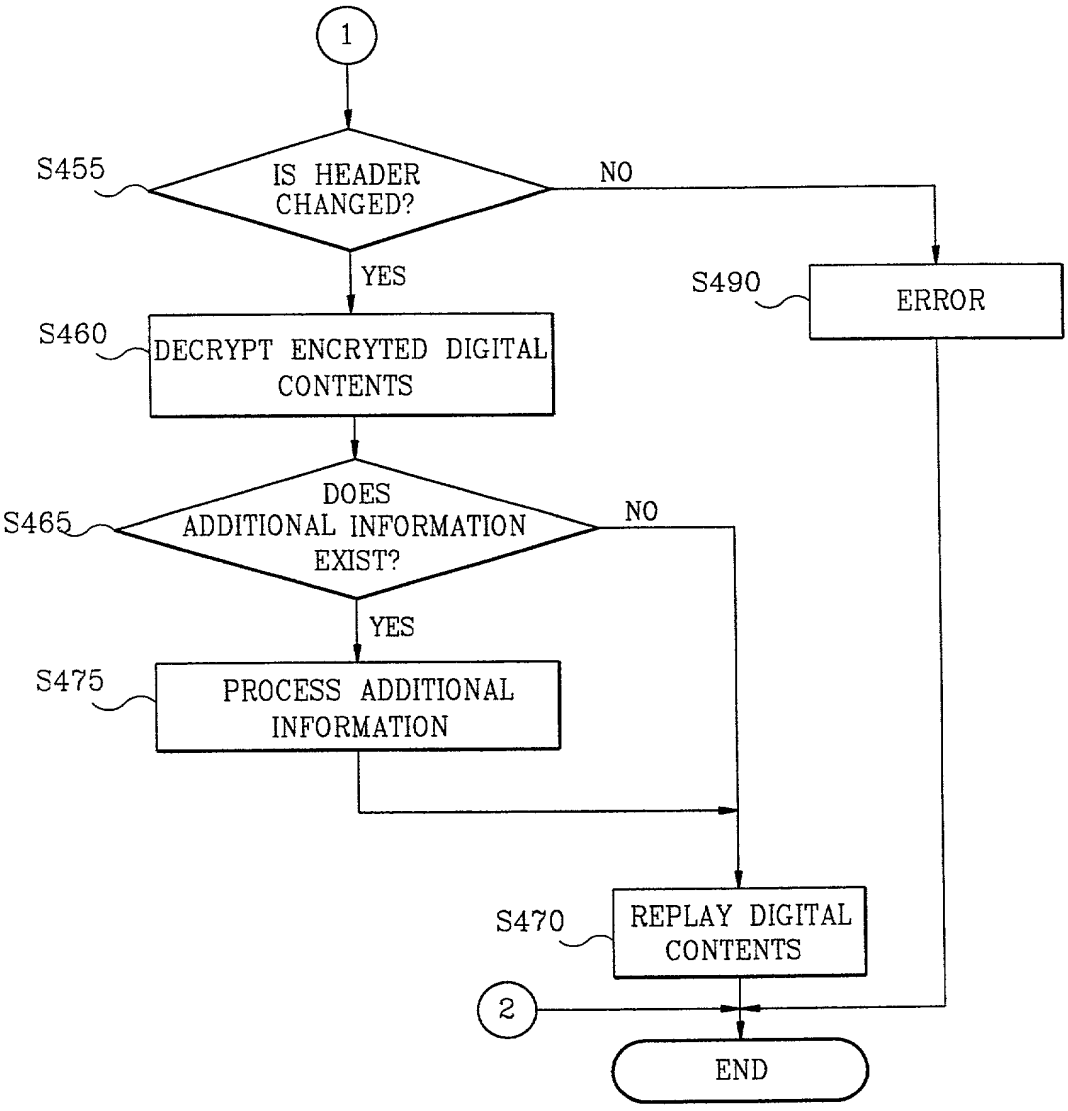

1
S455
IS HEADER CHANGED?
NO
YES
S490
ERROR
S460
DECRYPT ENCRYTED DIGITAL CONTENTS
S465
DOES ADDITIONAL INFORMATION EXIST?
NO
YES
S475
PROCESS ADDITIONAL INFORMATION
S470
REPLAY DIGITAL CONTENTS
2
END

FIG. 22

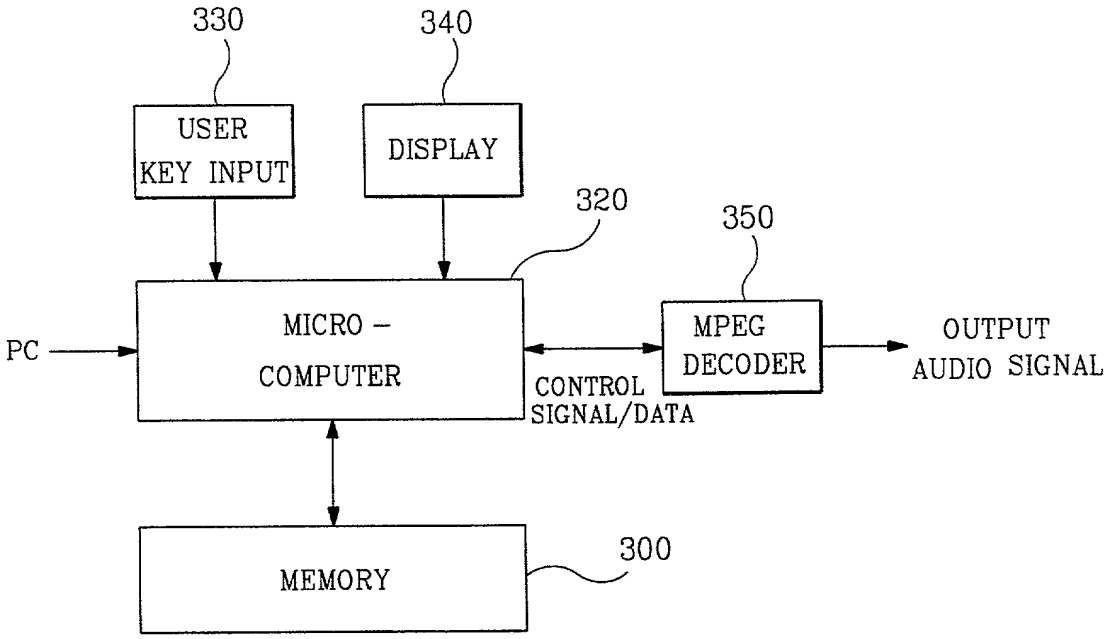

330
340
USER
KEY INPUT
DISPLAY
320
350
PC
MICRO –
COMPUTER
MPEG
DECODER
OUTPUT
AUDIO SIGNAL
CONTROL
SIGNAL/DATA
MEMORY
300

FIG. 23A

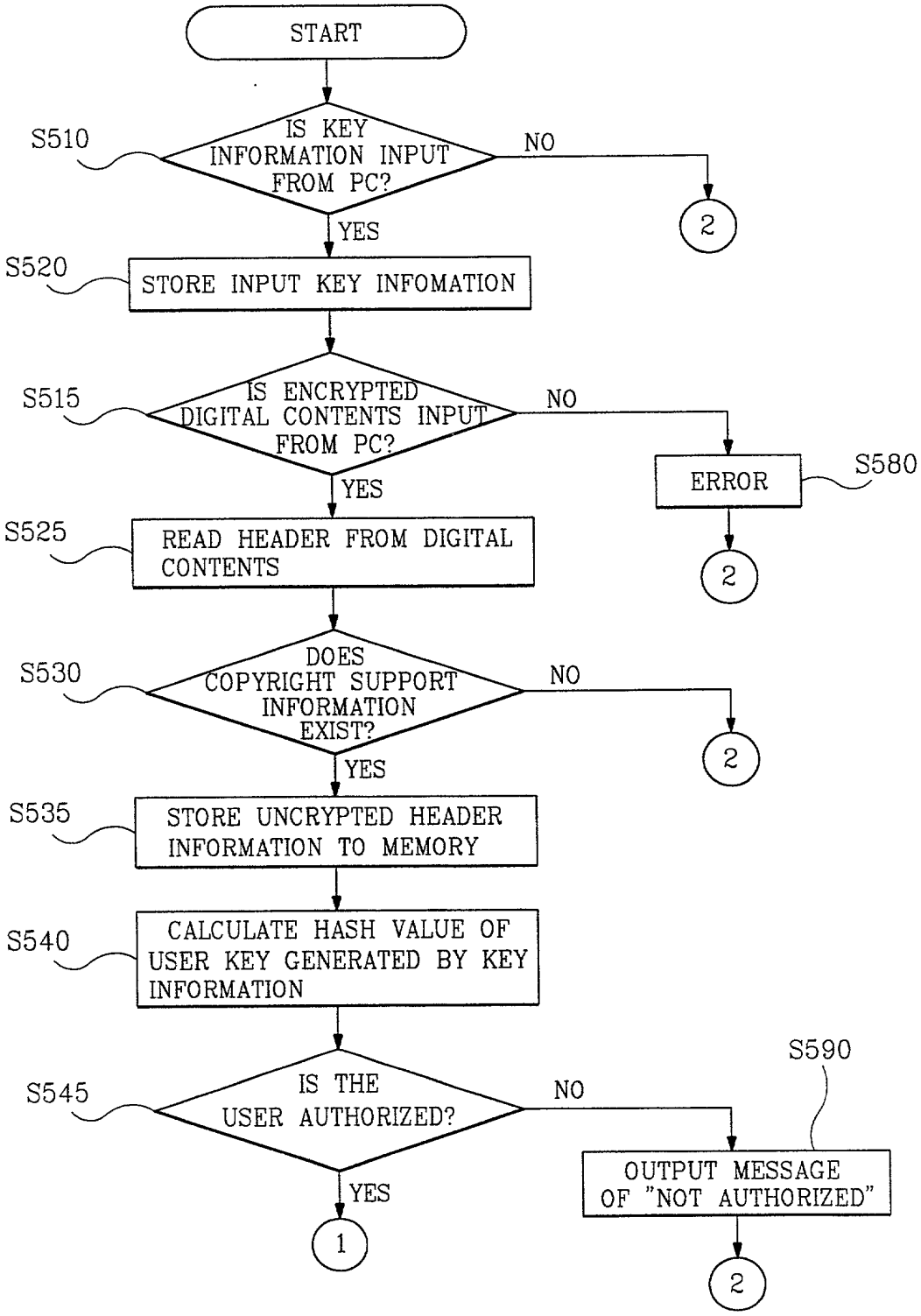
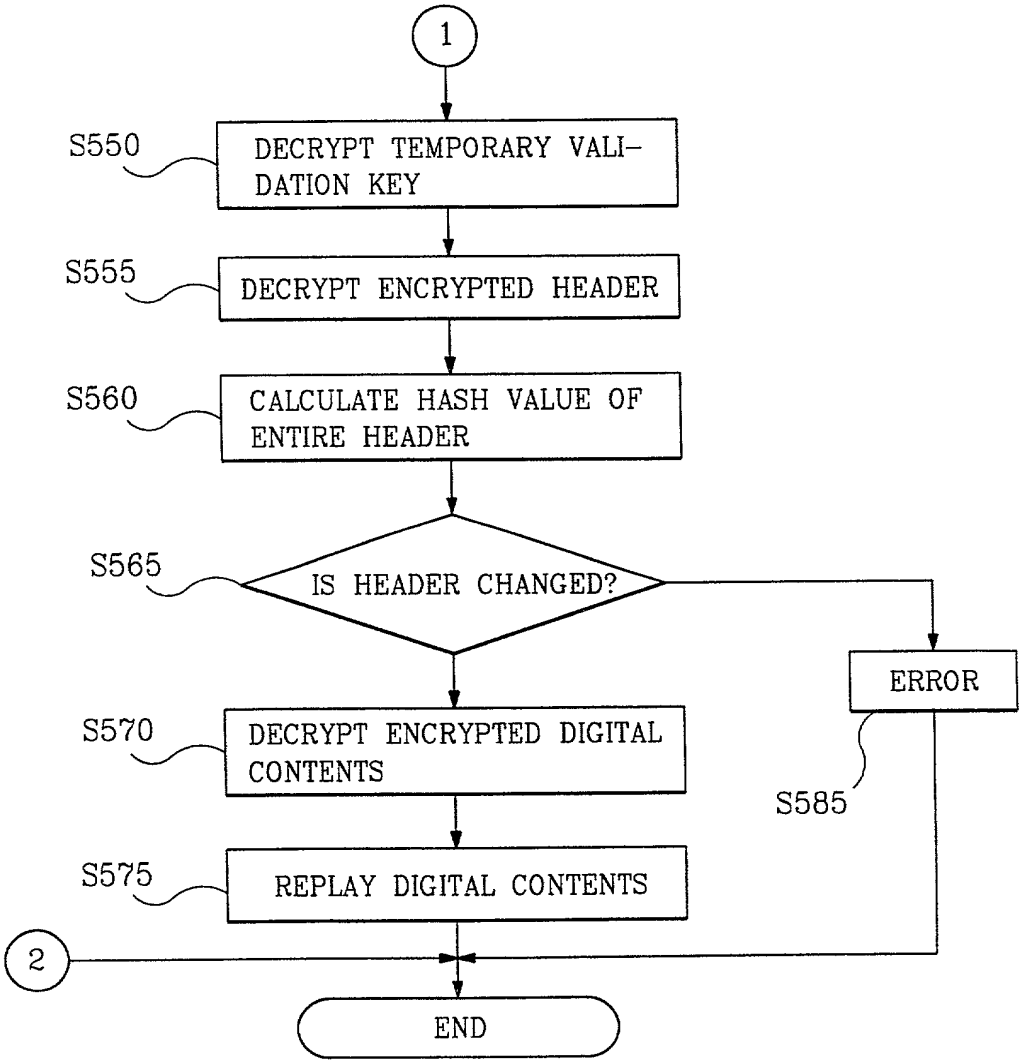

START
S510
IS KEY INFORMATION INPUT FROM PC?
NO
YES
2
S520
STORE INPUT KEY INFOMATION
S515
IS ENCRYPTED DIGITAL CONTENTS INPUT FROM PC?
NO
YES
ERROR
S580
2
S525
READ HEADER FROM DIGITAL CONTENTS
S530
DOES COPYRIGHT SUPPORT INFORMATION EXIST?
NO
YES
2
S535
STORE UNCRYPTED HEADER INFORMATION TO MEMORY
S540
CALCULATE HASH VALUE OF USER KEY GENERATED BY KEY INFORMATION
S545
IS THE USER AUTHORIZED?
NO
YES
S590
OUTPUT MESSAGE OF "NOT AUTHORIZED"
1
2

FIG. 23B


1
S550
DECRYPT TEMPORARY VALI-DATION KEY
S555
DECRYPT ENCRYPTED HEADER
S560
CALCULATE HASH VALUE OF ENTIRE HEADER
S565
IS HEADER CHANGED?
ERROR
S585
S570
DECRYPT ENCRYPTED DIGITAL CONTENTS
S575
REPLAY DIGITAL CONTENTS
2
END

PTO/SB/01 (6/95)

DECLARATION

Docket No. _____

AS A BELOW NAMED INVENTOR, I hereby declare that:
My residence, post office address and citizenship are as stated next to my name.
I believe that I am the original, first and sole (*if only one name is listed below*), or an original, first and joint inventor (*if plural names are listed below*), of the subject matter which is claimed and for which a patent is sought on the invention entitled:

TITLE: The Digital Content Encryption Apparatus and Method Thereof

the specification of which either is attached hereto or otherwise accompanies this Declaration, or:

☐ was filed in the U.S. Patent & Trademark Office on _____ and assigned Serial No _____,

☐ and (*if applicable*) was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability and to the examination of this application in accordance with Title 37 of the Code of Federal Regulations §1.56. I hereby claim foreign priority benefits under Title 35, U.S. Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, or §119(e) of any United States provisional application(s), listed below and have also identified below any foreign applications for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

(Application Number)	(Country)	(Day/Month/Year filed)	Priority Claimed:
98-39808	Korea	24/09/1998	Yes [X] No [ ]
98-39809	Korea	24/09/1998	Yes [X] No [ ]
			Yes [ ] No [ ]

I hereby claim the benefit under Title 35, U.S. Code, §120, of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application(s) in the manner provided by the first paragraph of Title 35, U.S. Code, §112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, The Code of Federal Regulations, §1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)	(Filing Date)	(STATUS: patented, pending, abandoned)

I hereby appoint the following attorneys: Robert E. Bushnell, Reg. No. 27,774, and Michael D. Parker, Reg. No. 34,973, to prosecute this application and to transact all business in the U.S. Patent & Trademark Office connected therewith and with any divisional, continuation, continuation-in-part, reissue or re-examination application, with full power of appointment and with full power to substitute an associate attorney or agent, and to receive all patents which may issue thereon, and request that all correspondence be addressed to:

Robert E. Bushnell,
Attorney-at-Law
Suite 425, 1511 "K" Street, N.W.
Washington, D.C. 20005-1401

Payor No. 008439
Area Code: 202-638-5740

I HEREBY DECLARE that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 U.S. Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST OR SOLE INVENTOR: En-Seung, KANG
Citizenship: KOREA
Inventor's signature: En-Seung KANG
Date: Dec. 1, 1998
Residence & Post Office Address: 1-103 Samho APT., Bangbaebon-dong
Seocho-ku, Seoul, Korea

FULL NAME OF SECOND JOINT INVENTOR: Jin-Young, Byun
Citizenship: Korea
Inventor's signature: Jin young Byun
Date: Dec. 1, 1998
Residence & Post Office Address: Software Center, Abkujung Building
599-4 Sinsa-dong, Kangnam-ku, Seoul, Korea

FULL NAME OF THIRD JOINT INVENTOR: _____
Citizenship: _____
Inventor's signature: _____
Date: _____
Residence & Post Office Address:

FULL NAME OF FOURTH JOINT INVENTOR: _____
Citizenship: _____
Inventor's signature: _____
Date: _____
Residence & Post Office Address:

☐ Additional inventors are being named on separately numbered sheets attached hereto.